MARONDERA RURAL DISTRICT COUNCIL I.T POLICY

1. Introduction

Marondera Rural district Council manages its Information Assets and Information Technology (IT) Assets with due diligence, due care and takes appropriate measures to safeguard these assets to ensure continued delivery of services and products.

Objective

Marondera Rural district Council's senior management sets the direction to manage security risks and protect the Organization's Information Assets and IT Assets. Marondera Rural district Council's Information Technology Policy(the "Policy") defines broad guidance for all the security controls required to maintain Marondera Rural district Council's business operations in compliance with its security policies, standards and guidelines as well as legal and regulatory requirements where applicable.

Information Assets and IT Assets are among Marondera Rural district Council's most vital assets to support its business activities.
Marondera Rural district Council's commitment to the protection of its Information Assets and IT Assets is a key component to support the Organisation's mission to deliver quality services and products to its clients.

The Policy contains a set of comprehensive security policy statements which will serve to provide guidance for the development of additional security policies, directives, standards, processes and procedures.

The Policy takes precedence over all previous published security policies with respect to information security.

2. Scope

The Policy applies to:

- All Information Assets and IT Assets owned or managed by Marondera Rural district Council and used internally or externally.
- All Users of Marondera Rural district Council IT Assets.

3. Roles and Responsibilities

3.1 Policy Owner

As the Policy Owner, the Chief Executive Officer is accountable for overall effectiveness and enforcement of the Policy throughout Marondera Rural district Council and for ensuring that the Policy continues to address Marondera Rural district Council's business needs.

3.2 Policy Custodian

As the Policy Custodian, the Chief Executive Officer is responsible for maintaining the currency of the Policy and for ensuring thatthe Policy continues to address Marondera Rural district Council's business

needs.

3.3 Information Owners

Information Owners are responsible for the following:

- Defining the security requirements to protect the Information Assets under their responsibility.
- Identifying the classification level of the Information Assets based on its degree of sensitivity.
- Ensuring the identification and management of security risks.
- Authorizing access to Users with a specific business need.
- Authorizing the secure disposal of the Information Assets.
- Ensuring compliance of the IT security policies, directives, standards, processes and procedures.

3.4 Information Custodians

Information Custodians are responsible for the following:

- Ensuring that the protection measures determined by the security baseline, information classification level or by the Information Owners are applied.
- Monitoring information security safeguards to ensure their proper implementation.
- Supporting operations and maintenance activities associated with the IT Assets.

- Administering logical and physical access to the Information Assets as authorized by the Information Owner.
- Administering the disposal of the Information Assets as authorized by the Information Owner in accordance with information classification levels and record retention requirements.
- Ensuring that Users are adequately trained to comply with the Policy.

Information Custodians can also be delegated authority by the Information Owner to perform essential functions under the Information Owner's responsibilities.

3.5 Users

All Users are responsible for the following:

- Becoming familiar and complying with the Policy, other relevant Marondera Rural district Council's IT policies, directives, standards, processes and procedures according to their responsibilities.
- Protecting Marondera Rural district Council's Information Assets against unauthorized access, modification, disclosure or loss, in a consistent and reliable manner.
- Using Marondera Rural district Council's IT Assets for business purposes and as outlined in their job requirements and description and other related policies, and conducting their business activities with diligence, and to adhere to the Policy.▪ Adhering to Information Owner's and Information Custodian's

  instructions and guidelines;
- Promptly reporting compliance issues and breaches of the Policy to the Chief Executive Officer or his/her delegates.

4. Implementation

CEO is responsible to implement the Policy in the departments/ business unit(s) under their responsibility and to ensure

that all Users under their supervision are aware of the Policy and that it is

applied when conducting their business activities.

5. Supporting Documentation

The Policy should be read in conjunction with other Marondera Rural district Council's security policies and standards, which provide specific protocol for the implementation of the Policy.

6. Policy Statements

In order to provide enterprise-wide guidance and consistency, Marondera Rural district Council has issued the policy statements described in this section. These statements may be supported by additional security policies, directives, standards, processes and procedures as required.

6.1 Information Classification

Information Assets must be used for Marondera Rural district Council's business purposes. All Information Assets, regardless of their form or format, which are created or used in support of Marondera Rural district Council's business, must be protected in a manner commensurate with their value, sensitivity, criticality and risk of loss or compromise.

The Information Assets must be classified on the basis of the classification level defined by the Information Owners and according to the confidentiality, integrity and availability criteria.

6.2 Security Risk Management

Periodic risk assessment must be done on the Information Assets and IT Assets, for purposes of determining areas of improvement and recommending appropriate remediation.

Risk assessments can be conducted on any information system, including applications, servers, networks and any process or procedure by which these systems are administered and/or maintained.

The execution, development and implementation of remediation plans are the joint responsibility of the Information Owners, the Director, IT security and the departments responsible for the systems or areas being assessed.

6.3 Personnel Security

Based on the Marondera Rural district Council Code of Business Conduct and Ethics, Users must protect one of the Organisation's most valuable assets, its information. Users must adhere to the Policy at all times while using and/or handling Marondera Rural district Council's information systems. Based on Human Resource requirements, and in accordance with laws and regulations, employees may be required to sign a confidentiality agreement when it is necessary to protect Marondera Rural district

Council's Information Assets.

6.4 Access Control

Access to the Information Assets must be granted through the assignment of specific access privileges on a "need-to-know" basis, and with the least privileges required for the business needs. No access should be granted by default. A formal access management process must be established to ensure that only authorized Users have access to Marondera Rural district

Council's Information Assets.

6.5 Physical Security

Marondera Rural district Council facilities, offices, data centers, computer and telecommunications equipment rooms that house Marondera Rural district Council's IT infrastructures must be protected by a defined perimeter, security barriers and other appropriate physical access control measures.

The Chief Executive Officer is responsible for implementing and maintaining controls in Marondera Rural district Council IT datacenters to protect IT Assets from unauthorized access, damage or disruption.

All Users are responsible for physically protecting all the IT Assets entrusted to them.

6.6 IT Project Management Lifecycle

Information security should be integrated in the project management life cycle for Marondera Rural district Council IT projects and other projects affecting IT Assets, such as application development, acquisition,

integration and enhancements. Security requirements must be defined in the initial phase of a project to ensure compliance with Marondera Rural district Council's IT security policies and standards.

6.7 Operational Security Management

The security controls and responsibilities associated with the management of Marondera Rural district Council's operations must be documented and must include the segregation of duties. The integrity of

IT Assets must be maintained through the establishment of a formal change management process.

All technology and application infrastructures must be protected according

to the classification of information they support and aligned with Marondera Rural district Council's baseline security requirements. Third party software and hardware must be maintained at a level that provides the appropriate security. Software patches must be applied if they can reduce unacceptable security weaknesses. The security controls implemented must be monitored and audit logs enabled. Known vulnerabilities must be mitigated or associated risks should be explicitly accepted by the owner of the affected assets.

Information security incident management requires that security incidents be reported, documented and handled through a formal process.The Information Assets must be protected with backup copies according to information classification requirements or the minimum Marondera Rural district Council requirements and must comply with Marondera Rural district Council's Records Retention Policy.

7. Compliance

Marondera Rural district Council and all of its employees and Users must comply with applicable laws and regulations in the jurisdictions in which Marondera Rural district Council operates, including and without limitation, any and all privacy and related legislation and any security obligation requirements including the IT security policies, directives, standards and processes.

Appropriate management structure and controls must be implemented to ensure that regulatory requirements are satisfied when using information technology and when implementing new information systems, such as conducting regulatory and compliance reviews.

8. Exception Management

Exceptions to the Policy due to specific business, security or technical requirements or constraints must be managed by an exception handling process.

The exception handling process requires that an Exception Handling form be completed and submitted for approval to the IT Security Office. In this form a reason must be provided for deviation from the Policy, the risk(s) Marondera Rural district Council faces because of noncompliance, compensating controls that may help counter the threat, and a time period clearly showing when the exception will expire.

9. Sanctions

Any violation of the Policy may result in administrative and/or disciplinary action by Marondera Rural district Council, including those leading to dismissal or termination of employment or contract.

Disciplinary action may include:

- Verbal reprimand;
- Written reprimand;
- Restrictions on network, application or service access;
- Suspension or dismissal;
- Investigation leading to civil or criminal charges.

10. Policy review

A review of the Policy must be performed:

a) When a change is identified in the technology, business, and/or regulatory environment that may have an impact on Marondera Rural district Council's security exposure and posture;

b) By the Director, IT Security, on an annual basis at a minimum, and as required;Any changes to the Policy will have to be approved by the appropriate management channel before they are put into effect.

11. Questions and Comments

We invite you to send any questions, comments or suggestions you might have regarding the content of the Policy to the Director, IT security (itso@maronderardc.org.zw)

12. Effective Date

Policy's effective date: 21 March 2016

Policy's revision date: 07 March 2016

Policy's review date: 07 March 2016

13. Implementation Strategy

The Policy must be applied to:

a) All new IT Assets installed after the effective date of the Policy;

b) All IT Assets installed before the effective date of the Policy whenever they:

- Are reinstalled
- Undergo a substantial change
- Are of critical nature

14. Glossary of Terms

Information custodian

Individual responsible for overseeing and implementing the necessary safeguards to protect the information at the level classified by the Information Owner. Usually, this is a representative from an IT Department or information service provider.

Information owner

Individual with the authority for specified information and responsibility for establishing the controls for its generation, collection, processing, dissemination, and disposal. Usually this is the head of department or business unit responsible for creation of or modification of this information.

Email use policy

Email use policy

Context and overview

Key details

- Approved by board / management on: 7/03/2016
- Policy became operational on: 21/03.2016
- Next review date: 7/03/2016

Introduction

MRDC makes email available to its employees where relevant and useful for their jobs.

This email use policy describes the rules governing email use at the company. It also sets out how staff members are expected to behave when using email.

This policy should be read alongside other key policies. In particular, users should also read the company's data protection and internet use policies.

Why this policy exists

Email is a standard way to communicate in business. It's used widely and is arguably just as important as the telephone.

Like any technology, email can cause difficulties if used incorrectly or inappropriately. This email policy:

- Reduces the **security and business risks** faced by MRDC
- Lets staff know **how they are permitted to use company email**
- Ensures employees follow **good email etiquette**
- Helps the company **satisfy its legal obligations** regarding email use

Policy scope

This policy applies to all staff at MRDC who use the company email system.

It applies no matter where that email use takes place: on company premises, while travelling for business or while working from home.

It applies to use of company email on any device, no matter whether owned by the company or employee.

General email guidelines

Business email use

MRDC recognises that email is a key communication tool. It encourages its employees to use email whenever appropriate.

For instance, staff members may use email to:

- Communicate with customers or suppliers
- Distribute information to colleagues

Personal use of email

The company also recognises that email is an important tool in many people's daily lives. As such, it allows employees to use their company email account for personal reasons, with the following stipulations:

- Personal email use should be of a reasonable level and restricted to non-work times, such as breaks and during lunch.

- All rules described in this policy apply equally to personal email use. For instance, inappropriate content is always inappropriate, no matter whether it is being sent or received for business or personal reasons.

- Personal email use must not affect the email service available to other users.

  For instance, sending exceptionally large files by email could slow access for other employees.

- Users may access their own personal email accounts at work, if they can do so via our internet connection. For instance, a staff member may check their Yahoo or Google Mail during their lunch break.

Authorised users

Only people who have been authorised to use email at MRDC may do so.

Authorisation is usually provided by an employee’s line manager . It is typically granted when a new employee joins the company and is assigned their login details for the company IT systems.

Unauthorised use of the company’s email system is prohibited.

Employees who use company email without authorisation — or who provide access to unauthorised people — may have disciplinary action taken against them.

Key areas

Email security

Used inappropriately, email can be a source of security problems for the company.

Users of the company email system must not:

- Open email attachments from unknown sources, in case they contain a virus, Trojan, spyware or other malware.
- Disable security or email scanning software. These tools are essential to protect the business from security problems.
- Send confidential company data via email. The IT department can advise on appropriate tools to use instead.
- Access another user's company email account. If they require access to a specific message (for instance, while an employee is off sick), they should approach their line manager.

Staff members must always consider the security of the company's systems and data when using email. If required, help and guidance is available from line managers.

Users should note that email is not inherently secure. Most emails transmitted over the internet are sent in plain text. This means they are vulnerable to interception.

Although such interceptions are rare, it's best to regard email as an open communication system, not suitable for confidential messages and information.

Inappropriate email content and use

The company email system must not be used to send or store inappropriate content or materials.

It is important employees understand that viewing or distributing inappropriate content via email is not acceptable under any circumstances.

Users must not:

- Write or send emails that might be defamatory or incur liability for the company.

- Create or distribute any inappropriate content or material via email.

  Inappropriate content includes: pornography, racial or religious slurs, gender-specific comments, information encouraging criminal skills or terrorism, or materials relating to cults, gambling and illegal drugs.

  This definition of inappropriate content or material also covers any text, images or other media that could reasonably offend someone on thebasis of race, age, sex, religious or political beliefs, national origin, disability, sexual orientation, or any other characteristic protected by law.

- Use email for any illegal or criminal activities.

- Send offensive or harassing emails to others.

- Send messages or material that could damage MRDC's image or reputation.

Any user who receives an email they consider to be inappropriate should report this to their line manager or supervisor.

Copyright

MRDC respects and operates within copyright laws. Users may not use company email to share any copyrighted software, media or materials owned by third parties, unless permitted by that third party.

Employees must not use the company's email system to perform any tasks that may involve breach of copyright law.

Users should keep in mind that the copyright on letters, files and other documents attached to emails may be owned by the email sender, or by a third party. Forwarding such emails on to other people may breach this copyright.

Contracts and liability

Users must be careful about making commitments or agreeing to purchases via email.

An email message may form a legally-binding contract between MRDC and the recipient — even if the user has not obtained proper authorisation within the company.

Email disclaimer

The standard company email template includes an email disclaimer. Users must not remove or change this when they send messages.

Email marketing and bulk email

MRDC may use email to market to existing and potential customers. There is significant legislation covering bulk email and use of email for marketing. All email campaigns must be authorized. Users must not send bulk emails using the standard business email system.All questions about email marketing should be directed to the CEO.

Email best practice

Email etiquette

Email is often used to communicate with customers, partners and other important contacts. Although a relatively informal medium, staff should be aware that each email they send does affect the company's image and reputation.

It's a good idea to follow rules of good email etiquette. Users must:

- Not forward on chain emails or 'humorous' messages. These clog up people's in-boxes and some topics are not appropriate for the workplace

- Always use a meaningful subject line rather than leaving it blank or using a single word like 'hello'.

- Only use the 'important message' setting sparingly, for messages that really are important.

- Never ask recipients to send a 'message read' receipt. Many people find these annoying and not all email services support them.

- Not use ALL CAPITAL LETTERS in messages or subject lines. This can be perceived as impolite.

- Be sparing with group messages, only adding recipients who will find the message genuinely relevant and useful.

- Use the ‘CC’ (carbon copy) field sparingly. If someone really needs to receive a message, they should be included in the ‘to’ field.

- Use the ‘BCC’ (blind carbon copy) field to send group messages where appropriate. It stops an email recipient seeing who else was on the email.

Internal email

Email is a valid way to communicate with colleagues. However, it tends to be overused for internal communication.

Users should keep these points in mind when emailing colleagues:

- Would the issue be better addressed via a face-to-face discussion or telephone call?

- Is email the best way to send a document out for discussion? Often, it becomes very hard to keep track of feedback and versions.• It’s rarely necessary to ‘reply all’. Usually, it’s better to reply and then manually add other people who need to see a message.

Policy enforcement

Monitoring email use

The company email system and software are provided for

legitimate business use. The company therefore reserves the

right to monitor employee use of email.

Any such examinations or monitoring will only be carried out by authorised staff.

Additionally, all emails sent or received through the company's email system are part of official [company name] records. The company can be legally compelled to show that information to law enforcement agencies or other parties.

Users should always ensure that the business information sent via email is accurate, appropriate, ethical, and legal.

Potential sanctions

Knowingly breaching this email use policy is a serious matter. Users who do so will be subject to disciplinary action, up to and including termination of employment.

Employees, contractors and other users may also be held personally liable for violating this policy.

Where appropriate, the company will involve the police or other law enforcement agencies in relation to breaches of this policy.

However, the company is unlikely to take formal action if a user fails to adhere to the guidelines in the 'email best practice' section.

Internet use policy

Internet use policy

Context and overview

Key details

- Approved by board / management on: 7/03/2016
- Policy became operational on: 21/03/2016
- Next review date: 07/12/2016

Introduction

MRDC makes internet access available to its employees where relevant and useful for their jobs.

This internet use policy describes the rules governing internet use at the company. It also sets out how staff members are expected to behave when using the internet.

This policy should be read alongside other key policies. The company's data protection and email policies are particularly relevant to staff who use the internet.

Why this policy exists

The internet is a powerful tool that can bring significant benefits to [company name].

However, it's important every person at the company who uses the internet understands how to use it responsibly, safely and legally.

This internet use policy:

- Reduces the **online security risks** faced by [company name]
- Lets staff know what they **can and can't do** online
- Ensures employees **do not view inappropriate content** at work
- Helps the company **satisfy its legal obligations** regarding internet use

Policy scope

This policy applies to all staff at MRDC who use the company's internet on work time.

It applies no matter whether that internet access takes place on company premises, while travelling for business or while working from home.

It applies to use of the internet on any device that is owned by the company, or that is connected to any company networks or systems.

For example, it applies both to an employee using the internet at their desk, and to employees who connect their own tablets or smart phones to the company wireless network.

General internet guidelines

Internet use is encouraged

MRDC recognises that the internet is an integral part of doing business. It therefore encourages its employees to use of the internet whenever such use supports the company's goals and objectives.

For instance, staff members may use the internet to:

- Purchase office supplies
- Read or send emails
- Perform research
- Identify potential suppliers

There are many valid reasons for using the internet at work and the company certainly allows its employees to explore and take advantage of the internet's many advantages.

Personal internet use

The company also recognises that the internet is embedded in many people's daily lives. As such, it allows employees to use the internet for personal reasons, with the following stipulations:

- Personal internet use should be of a reasonable level and restricted to non-work times, such as breaks and during lunch.

- All rules described in this policy apply equally to personal internet use. For instance, inappropriate content is always inappropriate, no matter whether it is being accessed for business or personal reasons.

- Personal internet use must not affect the internet service available to other people in the company. For instance, downloading large files could slow access for other employees.

Authorised users

Only people who have been authorised to use the internet at MRDC may do so.

Authorisation is usually provided by an employee’s line manager. It is typically granted when a new employee joins the company and is assigned their login details for the company IT systems.

Unauthorised use of the company’s internet connection is prohibited.

Employees who use the internet without authorisation — or who provide access to unauthorised people — may have disciplinary action taken against them.

Key areas

Internet security

Used unwisely, the internet can be a source of security problems that can do significant damage to the company’s data and reputation.

- Users must not knowingly introduce any form of computer virus, Trojan, spyware or other malware into the company.

- Employees must not gain access to websites or systems for which they do not have authorisation, either within the business or outside it.

- Company data should only be uploaded to and shared via approved services. The IT department can advise on appropriate tools for sending and sharing large amounts of data.

- Employees must not steal, use, or disclose someone else’s login or password without authorisation.

Staff members must always consider the security of the company’s systems and data when using the internet. If required, help and guidance is available from line managers.

Inappropriate content and uses

There are many sources of inappropriate content and materials available online. It is important for employees to understand that viewing or distributing inappropriate content is not acceptable under any circumstances.

Users must not:

- Take part in any activities on the internet that could bring the company into disrepute.

- Create or transmit material that might be defamatory or incur liability for the company.

- View, download, create or distribute any inappropriate content or material.

  Inappropriate content includes: pornography, racial or religious slurs, gender-specific comments, information encouraging criminal skills or terrorism, or materials relating to cults, gambling and illegal drugs.

This definition of inappropriate content or material also covers any text, images or other media that could reasonably offend someone on the basis of race, age, sex, religious or political beliefs, national origin,

disability, sexual orientation, or any other characteristic protected by law.

- Use the internet for any illegal or criminal activities.

- Send offensive or harassing material to others.

- Broadcast unsolicited personal views on social, political, religious or other non-business related matters.

- Send or post messages or material that could damage Marondera RDC's image or reputation.

Copyright

MRDC respects and operates within copyright laws. Users may not use the internet to:

- Publish or share any copyrighted software, media or materials owned by third parties, unless permitted by that third party.

- Download illegal copies of music, films, games or other software, whether via filesharing services or other technologies.

Employees must not use the company's equipment, software or internet connection to perform any tasks which may involve breach of copyright law.

Policy enforcement

Monitoring internet use

Company IT and internet resources — including computers, smart phones and internet connections — are provided for legitimate business use.

The company therefore reserves the right to monitor use of the internet, to examine systems and review the data stored in those systems.

Any such examinations or monitoring will only be carried out by authorised staff.

Additionally, all internet data written, sent or received through the company's computer systems is part of official MRDC records. The company can be legally compelled to show that information to law enforcement agencies or other parties.

Users should always ensure that the business information sent over or uploaded to the internet is accurate, appropriate, ethical, and legal.

Potential sanctions

Knowingly breaching this internet use policy is a serious matter. Users who do so will be subject to disciplinary action, up to and including termination of employment.

Employees, contractors and other users may also be held personally liable for violating this policy.

Where appropriate, the company will involve the police or other law enforcement agencies in relation to breaches of this policy.

Social media policy

Social media policy

Context and overview

Key details

- Approved by board / management on: 7/01/2016
- Policy became operational on: 21/03/2016

Introduction

Employees of MRDC may be able to access social media services and social networking websites at work, either through company IT systems or via their own personal equipment.

This social media policy describes the rules governing use of social media at

MRDC.

It sets out how staff must behave when using the company's social media accounts. It also explains the rules about using personal social media accounts at work and describes what staff may say about the company on their personal accounts.

This policy should be read alongside other key policies. The company's internet use policy is particularly relevant to staff using social media.

Why this policy exists

Social media can bring significant benefits to MRDC, particularly for building relationships with current and potential customers.

However, it's important that employees who use social media within the company do so in a way that enhances the company's prospects.

A misjudged status update can generate complaints or damage the company's reputation. There are also security and data protection issues to consider.

This policy explains how employees can use social media safely and effectively.

Policy scope

This policy applies to all staff MRDC whouse social media while working — no matter whether for business or personal reasons.

It applies no matter whether that social media use takes place on company premises, while travelling for business or while working from home.

Social media sites and services include (but are not limited to):

- Popular social networks like **Twitter** and **Facebook**
- Online review websites like **Reevoo** and **Trustpilot**
- Sharing and discussion sites like **Delicious** and **Reddit**
- Photographic social networks like **Flickr** and **Instagram**
- Question and answer social networks like **Quora** and **Yahoo Answers**
- Professional social networks like **LinkedIn** and **Sunzu**

Responsibilities

Everyone who operates a company social media account or who uses their personal social media accounts at work has some responsibility for implementing this policy.

However, these people have key responsibilities:

- The [CEO**]** is ultimately responsible for ensuring that MRDC uses social media safely, appropriately and in line with the company's objectives,

- The [**CEO** is responsible for providing apps and tools to manage the company's social media presence and track any key performance indicators. They are also responsible for proactively monitoring for social media security threats.

General social media guidelines

The power of social media

MRDC recognises that social media offers a platform for the company to perform marketing, stay connected with customers and build its profile online.

The company also believes its staff should be involved in industry conversations on social networks. Social media is an excellent way for employees to make useful connections, share ideas and shape discussions.The company therefore encourages employees to use social media to support the company's goals and objectives.

Basic advice

Regardless of which social networks employees are using, or whether they're using business or personal accounts on company time, following these simple rules helps avoid the most common pitfalls:

- **Know the social network.** Employees should spend time becoming familiar with the social network before contributing. It's important to read any FAQs and understand what is and is not acceptable on a network before posting messages or updates.

- **If unsure, don’t post it.** Staff should err on the side of caution when posting to social networks. If an employee feels an update or message might cause complaints or offence — or be otherwise unsuitable — they should not post it. Staff members can always consult the [CEO] for advice.

- **Be thoughtful and polite.** Many social media users have got into trouble simply by failing to observe basic good manners online. Employees should adopt the same level of courtesy used when communicating via email.

- **Look out for security threats.** Staff members should be on guard for social engineering and phishing attempts. Social networks are also used to distribute spam and malware. Further details below.

- **Keep personal use reasonable.** Although the company believes that having employees who are active on social media can be valuable both to those employees and to the business, staff should exercise restraint in how much personal use of social media they make during working hours.

- **Don’t make promises without checking.** Some social networks are very public, so employees should not make any commitments or promises on behalf of [company name] without checking that the company can deliver on the promises. Direct any enquiries to the [CEO].

- **Handle complex queries via other channels.** Social networks are not a good place to resolve complicated enquiries and customer issues. Once a customer has made contact, employees should handle further communications via the most appropriate channel — usually email or telephone.

- **Don’t escalate things.** It’s easy to post a quick response to a contentious status update and then regret it. Employees should always take the time to think before responding, and hold back if they are in any doubt at all.

Use of company social media accounts

This part of the social media policy covers all use of social media accounts owned and run by the company.

Authorised users

Only people who have been authorised to use the company's social networking accounts may do so.

Authorisation is usually provided by the [CEO]. It is typicallygranted when social media-related tasks form a core part of an employee's job.

Allowing only designated people to use the accounts ensures the company's social media presence is consistent and cohesive.

Creating social media accounts

New social media accounts in the company's name must not be created unless approved by the [IT manger].

The company operates its social media presence in line with a strategy that focuses on the most-appropriate social networks, given available resources.

If there is a case to be made for opening a new account, employees should raise this with the [CEO].

Purpose of company social media accounts

MRDC's social media accounts may be used for many different purposes.

In general, employees should only post updates, messages or otherwise use these accounts when that use is clearly in line with the company's overall objectives.

For instance, employees may use company social media accounts to:

- Respond to **customer enquiries** and requests for help
- Share **blog posts, articles and other content** created by the company
- Share **insightful articles, videos, media and other content** relevant to the business, but created by others
- Provide fans or followers with **an insight into what goes on at the company**

Social media is a powerful tool that changes quickly. Employees are encouraged to think of new ways to use it, and to put those ideas to the [Chief Executive Officer].

Inappropriate content and uses

Company social media accounts must not be used to share or spread inappropriate content, or to take part in any activities that could bring the company into disrepute.

When sharing an interesting blog post, article or piece of content, employees should always review the content thoroughly, and should not post a link based solely on a headline.

Further guidelines can be found below.

Use of personal social media accounts at work

The value of social media

MRDC recognises that employees' personal social media accounts cangenerate a number of benefits. For instance:

- Staff members can make **industry contacts** that may be useful in their jobs
- Employees can discover content to help them **learn and develop** in their role
- By posting about the company, staff members can help to **build the business' profile** online

As a result, the company is happy for employees to spend a reasonable amount of time using their personal social media accounts at work.

Personal social media rules

Acceptable use:

- Employees may use their personal social media accounts for **work-related purposes** during regular hours, but must ensure this is for a **specific reason**

  . Social media should not affect the ability ofemployees to perform their regular duties.

- Use of social media accounts for non-work purposes is **restricted to non-work times,** such as breaks and during lunch.

Talking about the company:

- Employees should ensure it is clear that their social media account **does not represent MRDC's views** or opinions.

- Staff may wish to **include a disclaimer** in social media profiles: 'The views expressed are my own and do not reflect the views of my employer.'

Safe, responsible social media use

The rules in this section apply to:

- Any employees using company social media accounts
- Employees using personal social media accounts during company time

Users must not:

- Create or transmit material that might be **defamatory or incur liability** for the company.

- Post message, status updates or links to material or **content that is inappropriate**.

  Inappropriate content includes: pornography, racial or religious slurs, gender-specific comments, information encouraging criminal skills or terrorism, or materials relating to cults, gambling and illegal drugs.

  This definition of inappropriate content or material also covers any text, images or other media that could reasonably offend someone on the basis of race, age, sex, religious or political beliefs, national origin,

  disability, sexual orientation, or any other characteristic protected by law.

- Use social media for any **illegal or criminal activities**.

- Send **offensive or harassing material** to others via social media.

- Broadcast **unsolicited views** on social, political, religious or other non- business related matters.

- Send or post messages or material that **could damage [company name]’s image or reputation**.

- Interact with [company name]’s competitors in any ways which could be interpreted as being **offensive, disrespectful or rude**. (Communication with direct competitors should be kept to a minimum.)

- Discuss **colleagues, competitors, customers or suppliers** without their approval.

- Post, upload, forward or link to **spam, junk email or chain emails and messages**.

Copyright

MRDC respects and operates within copyright laws. Users may not usesocial media to:

- Publish or share any **copyrighted software, media or materials owned by third parties**, unless permitted by that third party.If staff wish to **share content published on another website**, they are free to do so if that website has obvious sharing buttons or functions on it.

- Share links to **illegal copies** of music, films, games or other software.

Security and data protection

Employees should be aware of the security and data protection issues that can arise from using social networks.

Maintain confidentiality

Users must not:

- Share or link to any content or information owned by the company that could be considered **confidential or commercially sensitive**.

  This might include sales figures, details of key customers, or information about future strategy or marketing campaigns.

- Share or link to any content or information owned by another company or person that could be considered **confidential or commercially sensitive**.

  For example, if a competitor's marketing strategy was leaked online, employees of MRDC should not mention it on social media.

- Share or link to data in any way that could breach the company's **data protection policy.**

Protect social accounts

- Company social media accounts should be **protected by strong passwords** that are changed regularly and shared only with authorised users.

- Wherever possible, employees should use **two-factor authentication** (often called mobile phone verification) to safeguard company accounts.

- Staff must not use a new piece of **software, app or service** with any of the company's social media accounts without receiving approval from the [CEO].

Avoid social scams

- Staff should watch for **phishing attempts**, where scammers may attempt to use deception to obtain information relating to either the company or its customers.Employees should never reveal sensitive details through social media channels. Customer identities must always be verified in the usual way before any account information is shared or discussed.

- Employees should **avoid clicking links** in posts, updates and direct messages that look suspicious. In particular, users should look out for URLs contained in generic or vague-sounding direct messages.

Policy enforcement

Monitoring social media use

Company IT and internet resources — including computers, smart phones and internet connections — are provided for legitimate business use.

The company therefore reserves the right to monitor how social networks are used and accessed through these resources.

Any such examinations or monitoring will only be carried out by authorised staff.

Additionally, all data relating to social networks written, sent or received through the company's computer systems is part of official MRDC records.

The company can be legally compelled to show that information to law enforcement agencies or other parties.

Potential sanctions

Knowingly breaching this social media policy is a serious matter. Users who do so will be subject to disciplinary action, up to and including termination of employment.

Employees, contractors and other users may also be held personally liable for violating this policy.

Where appropriate, the company will involve the police or other law enforcement agencies in relation to breaches of this policy.

Data Protection

Data protection policy

Context and overview

Key details

- Approved by board / management on: 7/03/2016
- Policy became operational on: 21/03.2016
- Next review date: 7/03/2016

Introduction

MRDC needs to gather and use certain information about individuals.

These can include customers, suppliers, 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.

Why this policy exists

This data protection policy ensures MRDC:

- Complies with data protection law and follow 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 Data Protection Act 1998 describes how organizations — including MRDC 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 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

People, risks and responsibilities

Policy scope

This policy applies to:

- The head office of Marondera RDC
- All branches of Marondera RDC
- All staff and volunteers of Marondera RDC
- All contractors, suppliers and other people working on behalf of Marondera RDC

It applies to all data that the company holds relating to identifiable individuals, even if that information technically falls outside of the Data Protection Act 1998. This can include:

- Names of individuals
- Postal addresses
- Email addresses
- Telephone numbers
- …plus any other information relating to individuals

Data Protection Risk

This policy helps to protect Marondera RDC 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.

Responsibilities

Everyone who works for or with Marondera RDC 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 MRDC meets its legal obligations.

- The CEO 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 MRDC

    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 **[Chief Executive Officer],** 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.
  - 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.

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.

- **[Marondera RDC] 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 storage

These rules describe how and where data should be safely stored. Questions about storing data safely can be directed to the Chief Executive Officer 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**, 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 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** (like a 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 [Marondera RDC] unless the business can make use of it.

- 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 Chief Executive Officer 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.

Data accuracy

The more important it is that the personal data is accurate, the greater the effort

[Marondera RDC] 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.

- [Marondera RDC] will make it **easy for data subjects to update the information** [Marondera RDC] 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.

Subject access requests

All individuals who are the subject of personal data held by [Marondera RDC] 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 [email address]. The data controller can supply a standard request form, although individuals do not have to use this.

Individuals will be charged £10 per subject access request. The data controller will aim to provide the relevant data within 14 days.

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

Disclosing data for other reasons

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

Under these circumstances, [Marondera RDC] will disclose 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.

Providing information

[Marondera RDC] 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.

Website privacy policy

Website privacy policy

Key details

This website privacy policy describes how [Marondera RDC] protects and makes use of the information you give the company when you use this website.

If you are asked to provide information when using this website, it will only be used in the ways described in this privacy policy.

This policy is updated from time to time. The latest version is published on this page. This website privacy policy was updated on: 7/03/2016If you have any questions about this policy, please email info@maronderardc.co.zw

Introduction

We gather and use certain information about individuals in order to provide products and services and to enable certain functions on this website.

We also collect information to better understand how visitors use this website and to present timely, relevant information to them.

What data we gather

We may collect the following information:

- Name and job title
- Contact information including email address
- Demographic information, such as postcode, preferences and interests
- Website usage data
- Other information relevant to client enquiries
- Other information pertaining to special offers and surveys

How we use this data

Collecting this data helps us understand what you are looking from the company, enabling us to deliver improved services.

Specifically, we may use data:

- For our own internal records
- To improve the services we provide
- To contact you in response to a specific enquiry
- To customise the website for you
- To send you emails about services, offers and other things we think might be relevant to you.
- To send you mailings or to call you about services, offers and other things we think might be relevant to you.
- To contact you via email, telephone or mail for market research reasons.

Cookies and how we use them

What is a cookie?

A cookie is a small file placed on your computer's hard drive. It enables our website to identify your computer as you view different pages on our website.

Cookies allow websites and applications to store your preferences in order to present content, options or functions that are specific to you. They also enable us to see information like how many people use the website and what pages they tend to visit.

How we use cookies

We may use cookies to:

- **Analyse our web traffic using an analytics package.** Aggregated usage data helps us improve the website structure, design, content and functions.

- **Identify whether you are signed in to our website.** A cookie allows us to check whether you are signed in to the site.

- **Test content on our website.** For example, 50% of our users might see one piece of content, the other 50% a different piece of content.

- **Store information about your preferences.** The website can then present you with information you will find more relevant and interesting.

- **To recognise when you return to our website.** We may show your relevant content, or provide functionality you used previously.

Cookies do not provide us with access to your computer or any information about you, other than that which you choose to share with us.

Controlling cookies

You can use your web browser's cookie settings to determine how our website uses cookies. If you do not want our website to store cookies on your computer or device, you should set your web browser to refuse cookies.

However, please note that doing this may affect how our website functions. Some pages and services may become unavailable to you.

Unless you have changed your browser to refuse cookies, our website will issue cookies when you visit it.

Security

We will always hold your information securely.

To prevent unauthorised disclosure or access to your information, we have implemented strong physical and electronic security safeguards.

We also follow stringent procedures to ensure we work with all personal data in line with the Data Protection Act 1998.

Links from our site

Our website may contain links to other websites.

Please note that we have no control of websites outside the [our domain] domain. If you provide information to a website to which we link, we are not responsible for its protection and privacy.

Always be wary when submitting data to websites. Read the site’s data protection and privacy policies fully.