INFORMATION TECHNOLOGY POLICIES OVERVIEW

Data Protection

Introduction

The company 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 the company:

- 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

Data Protection legislation in the jurisdictions in which we operate describes how organisations — including the company — 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 legislation is underpinned by principles which encompass the following about the manner in which data must be handled. 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

Our policies seek to address each of these principles.

Scope

- **People, risks and responsibilities**

This policy applies to:

• All branches of the company in all regions around the world

• All staff and volunteers of the company

• All contractors, suppliers and other people working on behalf of the company

It applies to all data that the company holds relating to identifiable individuals. This can include:

• Names of individuals

• Postal addresses

• Email addresses

• Telephone numbers

• Any other information relating to individuals

- **Data protection risks**

This policy helps to protect the company 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 the company 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 directors are ultimately responsible for ensuring that the company meets its legal obligations.

• The IT manager, is responsible for:

o Keeping the directors updated about data protection responsibilities, risks and issues.

o Reviewing all data protection procedures and related policies, in line with an agreed schedule.

o Arranging data protection training and advice for the people covered by this policy.

o Handling data protection questions from staff and anyone else covered by this policy.

o Dealing with requests from individuals to see the data the company holds about them (also called 'subject access requests').

o Checking and approving any contracts or agreements with third parties that may handle the company's sensitive data.

o Ensuring all systems, services and equipment used for storing data meet acceptable security standards.

o Performing regular checks and scans to ensure security hardware and software is functioning properly.

o 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:

o Approving any data protection statements attached to communications such as emails and letters.

o 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.

• The company 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 IT manager or data controller. 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.

• 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 and never shared between employees.

• If data is stored on removable media (like a CD, DVD, Memory Stick), 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. Employees will have access to the company's cloud storage facilities. Data should not be uploaded to a personal cloud storage or local storage location. Should you wish to give a client or third party access to files that are stored on a cloud storage facility, please alert the IT Staff who will arrange this on your behalf.

• 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.

• 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 the company 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.

• Sensitive Data must be encrypted before being transferred electronically. The IT Manager can explain how to send data to authorised 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 law requires the company 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 the company 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.
- The company will make it easy for data subjects to update the information the company 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 the company 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 info@wconsulting.co.za. The data controller can supply a standard request form, although individuals do not have to use this. 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, the company will disclose requested data. However, the data controller will ensure the request is legitimate, seeking assistance from the directors and from the company's legal advisers where necessary.

Providing information

The company 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.

Acceptable Use of Information Technology Systems

Introduction

This Acceptable Use Policy (AUP) for IT Systems is designed to protect the company, company employees, customers and other partners from harm caused by the misuse of company IT systems and company data. Misuse includes both deliberate and inadvertent actions.

The repercussions of misuse of company systems can be severe. Potential damage includes, but is not limited to, malware infection (e.g. computer viruses), legal and financial penalties for data leakage, and lost productivity resulting from network downtime.

Everyone who works at the company is responsible for the security of the company IT systems and the data on them. As such, all employees must ensure they adhere to the guidelines in this policy at all times. Should any employee be unclear on the policy or how it impacts their role they should speak to their manager or IT officer.

Definitions

“Users” is everyone who has access to any of the company’s IT systems. This includes permanent employees and temporary employees, contractors, agencies, consultants, suppliers, customers and business partners.

“Systems” means all IT equipment that connects to the corporate network or access corporate applications. This includes, but is not limited to, desktop computers, laptops, smartphones, tablets, printers, data and voice networks, networked devices, software, electronically-stored data, portable data storage devices, third party networking services, telephone handsets, video conferencing systems, and all other similar items commonly understood to be covered by this term.

Scope

This is a universal policy that applies to all Users and all Systems. For some Users and/or some Systems a more specific policy exists: in such cases the more specific policy has precedence in areas where they conflict, but otherwise both policies apply on all other points.

This policy covers only internal use of the company's systems, and does not cover use of company products or services by customers or other third parties.

Some aspects of this policy affect areas governed by local legislation in certain countries (e.g., employee privacy laws): in such cases the need for local legal compliance has clear precedence over this policy within the bounds of that jurisdiction. In such cases, local teams should develop and issue users with a clarification of how the policy applies locally.

Staff members at the company who monitor and enforce compliance with this policy are responsible for ensuring that they remain compliant with relevant local legislation at all times.

Use of IT Systems

All data stored on the company's systems is the property of the company. Users should be aware that the company cannot guarantee the confidentiality of information stored on any the company system except where required to do so by local laws.

The company's systems exist to support and enable the business. A small amount of personal use is, in most cases, allowed. However, it must not be in any way detrimental to users own or their colleague's productivity and nor should it result in any direct costs being borne by the company other than for trivial amounts (e.g., an occasional short telephone call).

The company trusts employees to be fair and sensible when judging what constitutes an acceptable level of personal use of the company's IT systems. If employees are uncertain they should consult their manager.

Any information that is particularly sensitive or vulnerable must be encrypted and/or securely stored so that unauthorised access is prevented (or at least made extremely difficult). However, this must be done in a way that does not prevent–or risk preventing–legitimate access by all properly-authorized parties.

The company can monitor the use of its IT systems and the data on it at any time. This may include (except where precluded by local privacy laws) examination of the content stored within the email and data files of any user, and examination of the access history of any users. The company reserves the right to regularly audit networks and systems to ensure compliance with this policy.

Data Security

If data on the company's systems is classified as confidential this should be clearly indicated within the data and/or the user interface of the system used to access it. Users must take all necessary steps to prevent unauthorised access to confidential information.

Users are expected to exercise reasonable personal judgement when deciding which information is confidential.
Users must not send, upload, remove on portable media or otherwise transfer to a non-the company system any information that is designated as confidential, or that they should reasonably regard as being confidential to the company, except where explicitly authorised to do so in the performance of their regular duties.

Users must keep passwords secure and not allow others to access their accounts. Users must ensure all passwords comply with industry standard safe passwords. Minimum 8 characters in length, contain upper and lower case characters, include 1 or more non-word character.

Users who are supplied with computer equipment by the company are responsible for the safety and care of that equipment, and the security of software and data stored it and on other the company systems that they can access remotely using it.

Because information on portable devices, such as laptops, tablets and smartphones, is especially vulnerable, special care should be exercised with these devices: sensitive information should be stored in encrypted folders only. Users will be held responsible for the consequences of theft of or disclosure of information on portable systems entrusted to their care if they have not taken reasonable precautions to secure it.

All workstations (desktops and laptops) should be secured with a lock-on-idle policy active after at most 10 minutes of inactivity. In addition, the screen and keyboard should be manually locked by the responsible user whenever leaving the machine unattended. Pressing the key combination CTRL-ALT-DEL will instantly take you to a screen that will allow you to lock any Windows desktop system.

Users who have been charged with the management of those systems are responsible for ensuring that they are at all times properly protected against known threats and vulnerabilities as far as is reasonably practicable and compatible with the designated purpose of those systems.

Users must at all times guard against the risk of malware (e.g., viruses, spyware, Trojan horses, rootkits, worms, backdoors) being imported into the company's systems by whatever means and must report any actual or suspected malware infection immediately. The company provides antivirus software and this is required to be installed on all users' systems and this may not be removed or disabled.

Unacceptable Use

All employees should use their own judgment regarding what is unacceptable use of the company's systems. The activities below are provided as examples of unacceptable use; however, it is not exhaustive. Should an employee need to contravene these guidelines in order to perform their role, they should consult with and obtain approval from their manager before proceeding.

- All illegal activities. These include theft, computer hacking, malware distribution, contravening copyrights and patents, and using illegal or unlicensed software or services. These also include activities that contravene data protection regulations.

- All activities detrimental to the success of the company. These include sharing sensitive information outside the company, such as research and development information and customer lists, as well as defamation of the company.

- All activities for personal benefit only that have a negative impact on the day-to-day functioning of the business. These include activities that slow down the computer network (e.g., streaming video, playing networked video games).

• All activities that are inappropriate for the company to be associated with and/or are detrimental to the company's reputation. This includes pornography, gambling, inciting hate, bullying and harassment.

• Circumventing the IT security systems and protocols which the company has put in place.

Enforcement

The company will not tolerate any misuse of its systems and will discipline anyone found to have contravened the policy, including not exercising reasonable judgment regarding acceptable use. While each situation will be judged on a case-by-case basis, employees should be aware that consequences may include the termination of their employment.

Use of any of the company's resources for any illegal activity will usually be grounds for summary dismissal, and the company will not hesitate to cooperate with any criminal investigation and prosecution that may result from such activity.

Security considerations

Employees are to ensure that they take all necessary precautions to safeguard the IT equipment in their possession. This includes all laptops, data access devices, cell phones and tablets.

When you are in the office, ensure that where your laptop is equipped with a locking mechanism that you secure it to your desk with the security cable and lock supplied. Where you have an office, ensure that you also lock your office. Do not store laptops in office cupboards or desk drawers;

Where IT equipment is to be used outside of the office, it should be transported in the locked boot of a motor vehicle. Laptops are not to be left unattended in a vehicle. If you must leave them in the vehicle, ensure that they are in a locked boot. On an aircraft, put your laptop in the overhead luggage compartment.

Do not check it in with your luggage, or on a small aircraft do not place it in the general luggage compartment in the nose or tail of the aircraft.
Where you use public transport and you feel that you may be prone to attack by mugging on your way to and from the office, consider if you need to take the laptop with you.

Always have back-ups of work/data left on your hard drive, and ensure that you do not keep the back-up storage device in your laptop bag.

Where IT equipment is lost or damaged in any way, the Company reserves the right to investigate the circumstances that led to such loss or damage and to take disciplinary action against the employee. Where the employee is found to have been negligent, this action may also include recovery of costs related to the loss from the employee.