Information Technology Policy & Procedures

Introduction

The WMF Consulting IT Policy and Procedure Manual provides the policies and procedures for selection and use of IT within the business which must be followed by all staff, including contractors – herein collectively referred to as employees. It also provides guidelines WMF Consulting will use to administer these policies, with the correct procedure to follow.

WMF Consulting will keep all IT policies current and relevant. Therefore, from time to time it will be necessary to modify and amend some sections of the policies and procedures, or to add new procedures.

Any suggestions, recommendations or feedback on the policies and procedures specified in this manual are welcome.

These policies and procedures apply to all employees globally.

Bring Your Own Device Policy

At WMF Consulting we require employees to (at a minimum) supply their own mobile phone and a personal computer/laptop on a Windows 10 operating system. Apple/Macintosh laptops/computers are incompatible with most programs used in our business applications so are not suitable to meet the requirements of this policy. Employees must have access to the full Microsoft Office 2024 suite, advanced .pdf editing programs, TimeDoctor software and Microsoft Windows Defender antivirus software.

We encourage you to read this document in full and to act upon the recommendations. This policy should be read and carried out by all employees.

Purpose of the Policy

This policy provides guidelines for the use of personally owned personal computers, laptops, smart phones and tablets for business purposes. All employees who use or access WMF Consulting's technology equipment and/or services are bound by the conditions of this Policy.

Procedures

Registration of personal mobile devices for business use

Personal mobile devices can only be used for the following business purposes:

- Email access;
- Business internet access; and
- Business telephone calls

Each employee who utilises personal mobile devices agrees:

- Access to business emails will be limited to your business email address and not any client business email addresses;
- Use of business emails on personal mobile devices must be encrypted;
- Not to download or transfer business sensitive information to the device. Sensitive information includes Employee IP and Confidential Information as defined in your employment contract;
- Not to use the registered mobile device as the sole repository for WMF Consulting's information. All business information stored on mobile devices should be backed up;
- To make every reasonable effort to ensure that WMF Consulting's information is not compromised through the use of mobile equipment in a public place. Screens displaying sensitive or critical information should not be seen by unauthorised persons and all registered devices should be password protected;
- Not to share the device with other individuals to protect the business data access through the device;

- To abide by WMF Consulting's internet policy for appropriate use and access of internet sites etc.;
- To notify WMF Consulting immediately in the event of loss or theft of the registered device;
- Not to connect USB memory sticks from an untrusted or unknown source to equipment used for business purposes;

All employees who have a registered personal mobile device for business use acknowledge that the business:

- Owns all intellectual property created on the device;
- Can access all data held on the device, including personal data;
- Will regularly back-up data held on the device;
- Will delete all data held on the device in the event of loss or theft of the device;
- Has the right to deregister the device for business use at any time.

Keeping mobile devices secure

The following must be observed when handling mobile computing devices (such as laptops and tablets):

- Mobile computer devices must never be left unattended in a public place, or in an unlocked house, or in a motor vehicle, even if it is locked. Wherever possible they should be kept on the person or securely locked away
- Cable locking devices should also be considered for use with laptop computers in public places, e.g. in a seminar or conference, even when the laptop is attended
- Mobile devices should be carried as hand luggage when travelling by aircraft.

Breach of this policy

Any breach of this policy will be referred to Luke Mellar who will review the breach and determine adequate consequences, which can include termination of employment.

Indemnity

WMF Consulting bears no responsibility whatsoever for any legal action threatened or started due to conduct and activities of staff in accessing or using these resources or facilities. All staff indemnify WMF Consulting against any and all damages, costs and expenses suffered by WMF Consulting arising out of any unlawful or improper conduct and activity, and in respect of any action, settlement or compromise, or any statutory infringement. Legal prosecution following a breach of these conditions may result independently from any action by WMF Consulting.

Information Technology Security Policy

Purpose of the Policy

This policy provides guidelines for the protection and use of information technology assets and resources within the business to ensure integrity, confidentiality and availability of data and assets.

Procedures

Physical Security

All security and safety of personal computers, laptops, notebooks, tablets and mobile phones will be the responsibility of the employee. Each employee is required to use password locks on their devices and to ensure the asset is kept safely at all times to protect the security of the asset.

Information Security

All information, data, files and documents relating to the business are to be stored on WMF Consulting's servers, our service providers' servers (e.g. where proprietary CRMs are utilised by clients) or Cloud based document storage system (which may change between different client businesses).

Employees are responsible for deleting documents containing business sensitive information that are automatically downloaded into local folders before being saved to business servers/cloud storage.

All technology that has internet access must have anti-virus software installed. It is the responsibility of the employee to install all anti-virus software and ensure that this software remains up to date on all technology used by the business.

All information used within the business is to adhere to the privacy laws and the business's confidentiality requirements. Any breach of this policy will be referred to Luke Mellar who will review the breach and determine adequate consequences, which can include termination of employment.