**Mobile and Personal Devices**

**Doc A6.2**

**Version: 1.0**

Publication Date: January 01, 2019

Current Status: Published

Author(s): Michael Woolard

Last Reviewed: Michael Woolard

**Table of Contents**

1 Scope 3

1.1 Responsibilities 3

2 Mobile Devices 3

2.1 Company Mobile Phones 3

2.2 USB Flash Drives 4

2.3 Laptop Computers 4

2.4 Reporting lost / stolen devices 4

2.5 PINs and Passcodes 4

2.6 Remote Access 4

3 Bring Your Own Device (BYOD) and Personal Devices 4

4 Document Control and Approval 6

4.1 Distribution 6

4.2 Version Information 6

# Scope

This document describes the policies related to mobile devices and teleworking within Wacky Widget.

## Responsibilities

Directors and managers are responsible for ensuring the provisions of this document are understood and adhered to by all staff and others as appropriate.

The Risk and Compliance Manager is responsible for developing and maintaining this procedure.

# Mobile Devices

This policy is applicable to all mobile devices, including but not limited to laptops, tablets, and mobile phones, that connect to, upload to or receive from the Wacky Widget network or systems.

* Equipment should be in your possession, locked or monitored at all times when you are outside of the Wacky Widget offices.
* No company data, of any classification, may be transmitted over a device connected to an unsecured public wireless network
* Portable IT devices should not be left unlocked, in the office overnight
* Loan equipment should always be returned at the end of the day, unless otherwise agreed.
* Avoid the risk of screen activity being overlooked by unauthorised persons.

Users are encouraged to ask the Security team for guidance if they are in any doubt of the requirements of this policy or its implementation

Wacky Widget reserves the right to remove or prevent such access to a specific user in line with this policy if there is any doubt as to ability of the user to comply with this policy.

## Company Mobile Phones

Employees may store personal data on company mobile phones.

Wacky Widget reserves the right to delete personal data from any company device, at any time. If the phone is believed to be lost or stolen, Wacky Widget will initiate a remote wipe of the device. Users must not disable or interfere with these controls.

## USB Flash Drives

Only USB flash drives that have been encrypted by Wacky Widget Internal IT may be used for storing Company information.

USB flash drives received from 3rd parties must not be connected to any Wacky Widget equipment.

## Laptop Computers

All laptop computer hard-drives must be encrypted using a full disk encryption tool.

## Reporting lost / stolen devices

Lost or stolen mobile phones and other devices must be reported to the service desk or Internal IT as soon as possible, and within no more than 24 hours of the loss occurring.

This applies to all devices with access to Company systems – whether Company devices or BYOD.

## PINs and Passcodes

All mobile devices storing company data are required to have a lock screen password.

Mobile phones and tablets are configured to lock and erase contents after no more than 10 failed attempts.

Mobiles devices automatically lock after no more than 3 minutes on inactivity.

## Remote Access

Remote access, where provided for Staff to access Company servers and data from outside the office, is only permitted using Wacky Widget permitted encrypted VPN over the Internet.

# Bring Your Own Device (BYOD) and Personal Devices

Definition of “Personal Devices” includes but is not limited to the following equipment.

* Monitors
* Printers/Fax/Scanner
* External HDD/SSD
* External CD/DVD ROM
* USB Drive
* Wireless access points / switches / routers / misc network equipment
* Raspeberry Pi / Arduino / small computer related product
* Personal laptop and computers
* Personal mobile phones
* IoT devices

Personal devices may not use Wacky Widget’s secure wireless network, be plugged into a network port inside an Wacky Widget office, nor connected to a secure Wacky Widget network without Internal IT approval.

Personal devices may not connect to any Wacky Widget equipment or have any Wacky Widget equipment connect to it without Internal IT approval.

Personal devices cannot be considered for use unless

* There is a clear business purpose
* They are fully patched
* Contain endpoint protection software
* Internal IT approves it

Personal devices may connect to a guest wireless network for internet use only.

When requesting BYOD exception approval, you must agree to the following:

* Company data may only be stored on the device in a designated area controlled by Internal IT using control software approved by Internal IT.
* Company data may not be stored outside of the designated area circumventing the control software.
* You agree that control software and other software is installed on your device which will require storage, compute, network and potentially other resources to run.
* Wacky Widget reserves the right to delete any company or personal data from the designated area, at any time.  If the phone is believed to be lost or stolen, Wacky Widget will initiate a remote wipe of the designated area and related software. Users must not disable or interfere with these controls. Personal data outside of the designated area should not be affected by this.
* You agree to abide by the requirements of all relevant Company policies.
* You agree to be responsible for all call charges, data charges and other costs related to usage or ownership of your own phone for whatever purpose those charges are incurred.
* You agree that the company will not be liable for any personal data loss or device damage that may be directly or indirectly a consequence of your participation in the BYOD program.

Any attempts to connect your own device to the company’s systems without the proper approval is a disciplinary offence.

# Document Control and Approval

The Chief Information Security Officer is the owner of this document and is responsible for ensuring that this procedure is reviewed in line with the review requirements of the ISMS.

A current version of this document is available to all members of staff and is the published version.

Signature: Executive Manager Signature Date: 01.01.2019

## Distribution

|  |  |
| --- | --- |
| **Name** | **Role** |
| *Intranet* | *Distribution to all staff* |

## Version Information

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Date** | **Author(s)** | **Details** |
| 0.1 | 11/28/18 | M.Woolard | First draft |
| 0.2 | 12/07/18 | M.Woolard | Second draft |
| 1.0 | 01/01/19 | M.Woolard | First published |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# 