Shapinsay Development Trust

PORTABLE IT EQUIPMENT POLICY

Introduction

This policy is to ensure the proper control of the use and issue of Laptop, Handheld Personal Computers and Portable IT Equipment in the most efficient, secure and cost effective manner. Security and confidentiality matters are also addressed.

Criteria for Issue

Staff who have a need to use a computer, or access computer data whilst away from the office will be considered for the issue of a Laptop, Handheld Personal Computer or other Portable IT Equipment.

Subject to available technology, mobile devices will be selected, adapted, and configured to support users with special needs e.g. ultra-lightweight, large display, large font, text-to-speech, voice control, speech-to-text.

NB: Mobile devices have a higher life-cycle cost of ownership. They are inherently expensive to buy, have limited upgradeability, and are less robust than desktops. They are also more vulnerable to theft and damage. Additionally they may contain sensitive information.

Line managers will need to take account of these issues in deciding whether to support the issue of mobile devices to their staff. Managers are reminded that it is their duty to ensure that their Staff comply with Company policies.

Users will be required to complete the document at Annex A, accepting responsibility for the Laptop Personal Computer etc., and any additional equipment handed over at the time.

Data security is the responsibility of all staff as individuals, and failure to observe appropriate security measures and policies will be treated as Gross Misconduct / Gross Professional Misconduct.

Security Issues Particularly Pertinent to Portable Equipment

Laptop, Handheld Personal Computers and Portable IT Equipment are particularly vulnerable to both opportunist and planned theft. This may entail inconvenience, cost of replacement, and breach of confidentiality. Where loss has occurred due to negligence on behalf of the user this will be addressed in accordance with the company disciplinary policy.

Data Security

All laptops and PDAs will be issued with software to encrypt all data held on the hard drive.

Until the individual’s laptop or PDA is encrypted with encryption software, users must not copy any PID (Personally Identifiable Data) or Confidential Data onto the laptop. This includes data held in offline folders created as a result of:

- Synchronisation of any network drives;
- Synchronisation of any Microsoft Outlook, the standard folder structure within Microsoft Outlook and Personal Folders linked to Microsoft Outlook.

Additionally, all confidential information should be kept in password protected files. Both Microsoft Word and Excel can be set up to require a password to open them.

Physical Security

Users are required to take every reasonable precaution for the physical security of their Laptop, Handheld Personal Computers and Portable IT Equipment.

Most modern laptops are fitted with a strong point for attachment of Kingston Micro security cables. Where a laptop is to be left for any length of time in an “at risk” area, one of these cables should be fitted.

If the device is to be left in the user’s normal workplace, it should be placed in a secure cupboard or drawer when not in use.

At all other times when it is in the user’s custody, apart from when it is actually in use, it should be kept switched off, and as securely as possible.

Ideally equipment should not be left in cars, but when unavoidable it should be secured out of sight in the boot preferably before starting the journey.

[All equipment will be security etched with the Company’s main post code.]

[Insurance

Laptop, Handheld Personal Computers and Portable IT Equipment are not covered by Company Insurance. If loss of the equipment is found to be due to negligence then the person accepting the equipment might be held liable for the cost of a replacement. Users may wish to consider insurance to cover the equipment whilst in their care.]

Annex A

EQUIPMENT AND CONTENTS HANDOVER

Name of Staff Member (please print):

Staff Main Location:

Manager:

Portable Device Type:

Portable Device Asset Number:

Portable Device Serial Number:

In addition to the [EQUIPMENT DESCRIPTION], the following items have been handed over:

- User Manual for Device **Yes □** **No □**
- Copy of Policy **Yes □** **No □**
- Power Lead & Transformer **Yes □** **No □**
- Network Cable **Yes □** **No □**
- Modem Cable **Yes □** **No □**
- Telephone connection adapter **Yes □** **No □**
- Security Token Serial Number **Yes □** **No □**

General condition of items issued:

- I acknowledge receipt of the items listed above.
- I have checked the details and agree that they are correct.
- I agree to use this equipment in accordance with the relevant Company policies.
- I agree that I will not attempt to connect the device to any network other than that set up by the systems support department.
- I accept that Systems Support reserve the right to inspect the Laptop with the minimum of notice.

Signature: ______________________________ Date: ______________________