The Use of Portable Computer Devices, Mobile Phones and Removable Media

Introduction

Horizon Strategic Partners recognises that the use of portable computer devices and removable media which help staff in the performance of their duties is becoming more widespread. This guidance aims to support staff using these devices by ensuring they are aware of information and security issues.

Definitions:

Portable Computer Devices – this includes Horizon Strategic Partners supported laptops, notebooks, tablet computers, PDA's (personal digital assistants) and mobile phones.

Removable Data Storage Media – this includes any physical item that can be used to store and/ or move information and requires another device to access it. For example, CD, DVD, floppy disc, tape, or digital storage devices (flash memory cards, USB disc keys, and portable hard drives). Essentially anything you can copy, save and/or write data to which can then be taken away and restored on another computer.

Scope

This guidance applies to all Horizon Strategic Partners staff including temporary staff and volunteers.

Only authorised staff should have access to portable computer devices and digital storage devices such as flash cards, USB disc keys and portable hard drives.

Any member of staff allowing access to any unauthorised person deliberately or inadvertently may be subject to disciplinary action.

Use of Portable Computer Devices

DO …

- Store portable equipment securely when not in use
- Security mark portable equipment with a UV pen
- Install a BIOS password, where possible
- Ensure files containing personal or confidential data are adequately protected e.g. encrypted
- Ensure that PDA's are configured so that they lock after a maximum period of 5 minutes inactivity. Once locked the PDA should be set to require password authentication to resume use.
- Install password protected screensavers on laptops
- Use anti-virus software
- Regularly update anti-virus software
- Regularly apply windows updates

- Regular backups of the data stored on the portable equipment
- Be aware that software and any data files created by staff on Horizon Strategic Partners portable computer devices are the property of the Horizon Strategic Partners
- Report **immediately** any stolen portable equipment to the police and line manager
- Be aware that the security of your portable computer device is your responsibility and you should check your home and car insurance policies to ensure they cover for business use
- Ensure that when portable devices are required to be disposed of / re-issued the disposal procedures in Appendix A are followed.
- Ensure that portable devices are returned to Horizon Strategic Partners if you are leaving employment

DO NOT …

- Use your own portable computer device or digital storage device such as flash cards, USB sticks and portable hard drives) for Horizon Strategic Partners business unless authorised by IT Services.
- Leave portable equipment in places where a thief can easily steal them
- Leave portable equipment visible in the car when traveling between locations
- Leave portable equipment in an unattended car
- Leave portable equipment unattended in a public place
- Install unauthorised software or download software / data from the internet
- Disable the virus protection software
- Allow unauthorised personnel/friends/relatives to use portable equipment in your charge
- Delay in reporting lost or stolen equipment,
- Attach unauthorised equipment to the network
- Remove person identifiable information off site without authorisation from your Line Manager
- Access any Personal Data in an environment where your screen can be read by an unauthorised person.

Home Working

Home working is allowed and encouraged, but there are some important requirements.

- Make sure devices are protected at all times by a firewall, anti-virus and the latest security patches are being applied regularly.
- Do not connect Horizon owned devices to public wifi networks.
- On your own device, do not access Horizon related data on public Wifi networks (eg Costa Coffee, or BT OpenZone Wifi)
- Ensure any processing of PID is done without exposing the data to unauthorised people (eg family members, non-Horizon employees)
- Ensure that any devices with access to Horizon data are kept safe and secure when not in use (eg in a locked room, or in a locked bag)

Appendix A – Disposal / Re-issue of Horizon Strategic Partners Owned Portable Devices

When an item requires disposal or is no longer required i.e. a person is leaving employment then the following procedures should be followed:

Floppy Disks/ CD-Rom/ Tapes

These items should be re-used/ destroyed locally. If the items contain sensitive or confidential information this must be removed before re-issue or if requiring disposal they should be shredded / incinerated.

Laptops, USB sticks, PDA's etc:

These items can be re-issued within Horizon Strategic Partners but the asset register must be updated accordingly and any sensitive / confidential information removed. If the item is no longer required then it should be disposed of correctly.