Document name:	*Primary Eyecare Cheshire: Mobile computing guidelines*
Date created:	*13 March 2017*
Author:	*Jane Smellie*
Approved by:	

Requirement 318: Mobile computing guidelines

This document outlines the guidelines that should be followed by directors and subcontractors when using portable computer devices, mobile phones and removable media.

Definitions

Portable Computer Devices – this includes laptops, notebooks, tablet computers, smartphones 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 directors and subcontractors.

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

Any director or subcontractor allowing access to any unauthorised person deliberately or inadvertently may be subject to disciplinary action.

Directors or subcontractors should not use unauthorised portable devices or digital storage device (such as personal phones) for storing or communicating information.

Use of Portable Computer Devices

DO …

- Store portable equipment securely when not in use
- Set up access controls, for example a personal password, where possible
- Ensure files containing confidential company data are adequately protected e.g. encrypted

- Ensure that smartphones are configured so that they lock after a maximum period of 5 minutes inactivity. Once locked the smartphone should be set to require password authentication to resume use.
- Install password protected screensavers on laptops
- Use and regularly update anti-virus software
- Take regular backups of the data stored on the portable equipment
- Report immediately any stolen portable equipment to the police and the Information Governance Lead
- 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

DO NOT …

- Store patient identifiable data on a portable computer or removable storage device
- Leave portable equipment in places where vulnerable to theft
- Leave portable equipment visible in the car when travelling between locations
- Leave portable equipment in an unattended car
- Leave portable equipment unattended in a public place
- Disable the virus protection software
- Allow unauthorised personnel/friends/relatives to access company data in your charge
- Delay in reporting lost or stolen equipment