Mobile and Teleworking Policy

1. Introduction

Mobile Computing and Teleworking can bring about many benefits to our organisation. It allows for information to be available whilst working on the move, in remote or home working situations. It can improve the patient care experience and can contribute to the improvement of working lives. These benefits, however, also present a new set of risks. Information is no longer retained within the Company; it is moving around the town, the country and potentially even abroad on a variety of devices and through other communication channels.

We only have to read the newspapers or watch the news to hear stories of information on devices such as laptops and memory sticks that get lost or stolen. Given the confidential nature of the information that we hold, and the adverse impacts that may be caused if it is lost or stolen, it is imperative that the Company implements robust information security arrangements where mobile devices are to be used.

2. Purpose

The purpose of this policy is to promote good information security practices outside the immediate boundaries of our company headquarters in Sheffield.

The policy is aimed at enabling and supporting employees who intend to use and transfer manual and computer files between home, the office and the community.

3. Aims

The aims of this policy are:

- To ensure that the Company complies with its legal obligations under the Data Protection Act 2018 and the UK General Data Protection Regulation (UK GDPR)
- To promote the safe and secure use of mobile equipment in support of clinical and operational work of the Company
- To provide a secure working practice for personnel/employees who intend to use and transfer manual and computer files between home, the office and the community
- To ensure that Company resources provided to staff are not misused
- To ensure that the security of computer systems and the information they contain is not compromised in any way
- To prevent the Company's' reputation from being damaged by the inappropriate or improper use of its information resources.

4. Scope

The policy relates to any staff member (including temporary workers, locums and staff seconded or contracted from other organisations) who at any time removes information in any form from the premises of the Company where it is usually stored for mobile computing or home working purposes.

5. Definitions

Mobile Computing

Mobile computing is the term used when working from a non-fixed location using mobile devices.

Teleworking

Teleworking is the term used when work is carried out away from the normal places of work such as offices, factories and is performed in a fixed location, i.e. at home.

Mobile Devices

Mobile devices are portable computers defined as:

- Laptops, notebooks, palmtops, handheld computers, digital cameras
- Blackberries, Personal Digital Assistants (PDA's), mobile phones.

Removable Media

In computer storage, removable media refers to storage media which is designed to be removed from the computer without powering the computer off. Examples include:

- Optical discs (Blu-ray discs, DVDs, CDs)
- Memory cards (CompactFlash card, Secure Digital card, Memory Stick)

Some removable media readers and drives are integrated into computers, others are themselves removable. Removable media may also refer to some removable storage devices when they are used to transport or store data.

Examples include:

- USB flash drives
- External hard disk drives.

Encryption

Encryption means converting information using a code that prevents it being understood by anyone who isn't authorised to read it. Passwords only provide basic security, so the data is still quite easy to access

To read an encrypted file a key or password must be used to decrypt it.

Encryption software uses a complex series of embedded mathematical algorithms to protect and encrypt information. This process hides the data and prevents any inadvertent or unauthorised access.

Information Asset

Refer to operating systems, infrastructure, business applications, off-the-shelf products, services, user-developed applications, records and information.

6. Responsibilities

All Company staff, contractors working on behalf of the Company allocated a mobile device or any form of removable media must adhere to this policy.

The Senior Information Risk Owner (SIRO) is an Executive Director and is responsible for coordinating the development and maintenance of information risk management policies, procedures, and standards for the Company.

Information Asset Owner's (IAO's) are directly accountable to the Senior Information Risk Owner (SIRO) and must provide assurance that information risk is being managed effectively in respect of the information assets that they 'own'.

The Information Asset Administrator's (IAA's) will implement the organisation's information risk policy and risk assessment process for those information assets they support and will provide assurance reports to the relevant Information Asset Owner as necessary.

7. Use of Mobile Devices and Removable Media

- Mobile devices and removable media where applicable, must be fully encrypted in line with national NHS requirements
- Only authorised mobile devices and removable media may be used for Company business
- Mobile devices and removable media should never be used as the primary source of data. The source data should reside on the Company's managed central servers where the backup and security of this can be controlled
- Where the source data is portable like a DVD/CD, this must be held in a safe location and a record kept for reference
- Mobile devices and removable media must only be used where there is an identified business need relevant to your role and this has been agreed with line management

- Mobile devices and removable media must be kept secure at all times. Each individual is responsible for its physical protection against loss, damage, abuse or misuse. This includes when it is used, where it is stored, and how it is protected in transit

- Mobile devices, in particular laptops must regularly (recommended once a week) be connected to the Internet to allow updates to be picked up e.g. Antivirus and Windows updates.

- Mobile devices and removable media should always be kept with you or locked away when not in use.

- Mobile devices and removable media use should be kept to a minimum when used in public areas.

- Under no circumstances must personal/patient identifiable information be saved on home computers.

8. Teleworking/Mobile Computing

Company staff accessing information systems remotely (including from home computers); either to support business activities or as a function of their job roles must be authorised to do so by the responsible information owner.

The physical and logical controls that are available within the Serenta Homecare network and physical environment are not automatically available when working outside of that environment, as a result, there is an increased risk of information being subject to loss or unauthorised access. Mobile computing/Teleworking users must take necessary measures to protect sensitive information in these circumstances.

Unauthorised access to and tampering with a Mobile computing/Teleworking device, particularly if there are repeated opportunities for access, may:

- Lead to continuing (and undetected) compromise of information on the device itself

- Undermine security measures (including the encryption), intended to protect information on the device in the event of loss or theft

- Lead to the compromise of systems to which the device is connected, for example, networked systems that are accessed from the device under an approved remote access arrangement.

Guidelines

The impact of a breach of Mobile computing/Teleworking security may extend far more widely than the device itself.

When undertaking Mobile computing/Teleworking the following guidelines must be followed:

- When travelling, equipment (and media) must not be left unattended in public places. Portable computers should be carried as hand luggage when travelling

- When using a laptop, do not process personal or sensitive data in public places e.g. on public transport

- General access to the laptop for use by immediate household members is not permitted. The employee bears responsibility for the consequences should the access be misused

- Passwords or other access tokens for access to the Companys systems should never be stored on mobile devices where they may be stolen or permit unauthorised access to the information assets

- Security risks (e.g. of damage, loss or theft) may vary considerably between locations and this should be taken into account when determining the most appropriate security measures

- Sensitive data, including that relating to patients, stored on a Company laptop should be kept to the minimum required for its effective business use in order to minimise the risks and impacts should a breach occur.

9. Encryption

The NHS Chief Executive has directed that there must be no transfers of unencrypted Person identifiable data held in electronic format across the NHS, particularly when information is transferred across the internet, held on portable devices or any type of removable media. Serenta Homecare has chosen to align itself with this directive.

Our IT provider will therefore:

- encrypt all PC desktops and laptops

- encrypt other mobile devices such as USB sticks, PDA's etc. (where issued by the Company).

  Please note USB drives are automatically disabled and only permitted where absolutely necessary. Please submit a request to your line manager.

- Issue encrypted USB memory sticks where authorised by heads of departments.

10. Transporting Paper Based Records

The following principles apply to paper-based records containing personal-identifiable information or Company sensitive information.

- Paper records must only be taken off-site where a line manager has identified an authorised business need. It must be recorded what has been taken, why, where to and by whom

- Records must be transported in sealed containers e.g. secured envelope, locked briefcase or transit bag. Not carried 'loosely'

- If staff are required for business purposes to transport records in their vehicle, they must be kept out of sight in a locked boot and not left in the vehicle overnight

- The person handling the records holds the responsibility for their safety and ensuring they are kept secure at all times.

12. Incident Reporting

The loss of any Company data held in any format and any portable device or removable media containing personal identifiable data is deemed a serious untoward incident (SUI) and must be reported immediately to the relevant line manager.

13. Performance Monitoring

As part of the process for managing Information Governance this policy will be reviewed annually against the DSP Toolkit to identify key areas for continuous improvement.

The DSP Toolkit contains guidance on expected standards and key performance indicators, which together will be used to monitor the effectiveness of this policy and in particular the following requirement.

Date Approved: June 2026
Target Audience: All Serenta Homecare Staff
Review Date: June 2028
Author: Fran Beardsmore