BrisDoc Patient care by people who care

NHS

Mobile Computing Policy

Version:	Owner:	Created:
1.8	Debs Lowndes (Head of Information and Projects)	1st September 2012
Published:	**Approving Director:**	**Next Review**
15th November 2023	Nigel Gazzard (Managing Director)	1st November 2025

Contents

Introduction

This document covers the use of all mobile computing devices. This includes but is not restricted to laptops, notebooks, memory sticks, external hard drives, and mobile phones. The policy applies to all co-owners.

Portable computer equipment is now being used more and more within the NHS environment and the security of such equipment, and the confidentiality, integrity and availability of information accessed/held/stored on/by the equipment, can be difficult to maintain.

The security provided should be equivalent to that for on-site equipment used for the same purpose, taking account of the risks of working outside of the organisation's premises.

The Data Protection Act 1998, Information Security NHS Code of Practice and the Caldicott recommendations all, refer to, and cover, the requirement to ensure information that is transferred must be done so in a secure and confidential manner.

The use of portable and remote equipment also creates risks due to lack of physical security and environmental considerations. Therefore, users of portable equipment need to be made aware of the dangers of loss, damage and breaches of security/confidentiality that can occur to the information they have responsibility for on the portable equipment.

The use of portable devices creates particular risks in the following areas:

- Small size and portability increase risk of loss, breakage, theft, and unauthorised use.
- Connection to a PC or network increases virus and hacking vulnerabilities
- The Scope for installing additional hardware and software could lead to compromised security, licensing problems and increased support requirements.

This document should be read in conjunction with the Information Security Policy.

Document Purpose

This policy applies to all persons using BrisDocs computing equipment, connecting to the BrisDoc network or otherwise accessing, recording, storing or transferring BrisDoc data, and consequently applies regardless of whether or not the device is the personal property of the user.

A breach of security and/or confidentiality can occur very easily with the loss or misuse of portable equipment. The purpose of this document is to provide clear guidance for those BrisDoc co-owners using portable computer equipment at any site or any other location by ensuring they are aware of the information security issues.

Definition of a Portable Computer/Equipment

Portable computer/equipment covered under the requirements of this procedure can be any of the following:

- Laptop computer
- Home Computer
- Remote Access Token
- Mass Storage Devices – including discs, external hard drives and memory sticks
- Mobile Phones
- Tablet Computers

This policy will also be applicable to mobile phones which have a significant data-processing functionality including contact, organisers and camera functions. A basic mobile having a telephone register of calls is not covered by this policy, but one having an address book or calendar, email access with PC/network linking capabilities would fall within its scope.

All mobile devices must have a BrisDoc asset sticker on them and included in the appropriate asset register.

Staff are reminded of the General Data Protection Regulations regarding the storage of person identifiable data, regardless of whether it is being electronically processed, and therefore is not acceptable to store any service user details on any device unless it is adequately secured against unauthorised access.

Management Responsibilities

Before it is decided if a co-owner or a contractor can be allocated and use portable equipment, a risk assessment should be undertaken to identify any potential risks to the data/information, programmes, and the equipment/media.

BrisDoc's Programme and Service Director/Digital Lead is responsible for maintaining an asset register of who has portable equipment as detailed in Section 3.

The details should be logged on the asset register to include which co-owner or contractor has current responsibility for the portable equipment. All equipment will be signed out when allocated to a co-owner or contractor and signed in when returned to BrisDoc as appropriate. Either because the co-owner leaves employment, changes job and no longer needs the equipment or is off on long term sickness or extended annual leave, or the contractor ceases to work for BrisDoc.

The following should also be detailed in the asset register/log:

- Details of the equipment
- The information it holds
- The information it will hold &/or work to be carried out
- Equipment asset number
- Details of person 'loaning' the equipment
- Date Issued
- Date Returned

All unused assets will be held at Osprey Court or a safe location on site. Access to these assets will be limited to the Programme and Service Director/Digital Lead and Site/Service Managers/Team Managers.

The Site/Service Manager will ensure all staff using portable equipment is made aware of their personal responsibilities in line with General Data Protection Regulations (GDPR), their contract of employment, Confidentiality Code of Conduct and policies and procedures relevant to the security and confidentiality of personal information. The most relevant will be the Data Protection Policy and the Information Security Policy.

All co-owners and contractors will be issued with Fact Sheet, which sets out the content of this policy.

The additional risks surrounding the use of mobile computing, and the controls needed to minimise them will be covered in mandatory co-owner training. Co-owners should also be made aware of any special security features applicable to the equipment they will be using e.g., locking, SIM cards, setting file passwords as appropriate.

User Responsibilities

Each co-owner should have a signed a confidentiality clause as part of their contract of employment. This makes clear that all personal information must be treated carefully and must not be disclosed to unauthorised persons.

Within the management of BrisDocs assets especially portable devices each co-owner member will be asked to sign for receipt of the portable device, and to acknowledge that they have read, understood, and will comply with this policy.

- No other person must be able to access the equipment.
- Users must be aware they have personal responsibility for the equipment and all data/information accessed/held/stored on the equipment and accompanying media.
- All users of portable equipment must ensure they have read and understood this, Policy.
- Users must have a copy and understand their requirements detailed of the BrisDoc Confidentiality Code of Conduct.
- Users must be made aware of action to take in the event of the equipment being lost or stolen. Action required is detailed within this Policy in Section 9.

Physical Protection

- Portable computers/equipment are prone to rougher treatment than a desktop computer unit and are therefore more likely to breakdown or become damaged. All users should ensure they take care of the equipment in their care.

- Portable equipment must not be left unattended in any public places.

- Portable equipment (as defined above) must not be left unattended in open offices.

- It is normal for portable computer equipment to come with a purpose made carry case. These cases should always be used when transporting the equipment inside or outside BrisDoc premises.

- Portable equipment must be always kept in the possession of the co-owner. Therefore, the equipment must be removed from the car when the co-owner leaves the car unattended e.g., in car park.

- If the portable equipment has a removable disc which can hold data/information it is sometimes better to detach the two and transport separately e.g. equipment in carry case and disc in inside pocket of coat.

- Ensure that any equipment is always kept within the environmental ranges detailed with the user guide that accompanies the equipment. This also applies to the media that may also be carried with the equipment e.g. CD, memory stick or other media. There have been situations where data has been corrupted on a hard disc when there was a rapid fluctuation of temperature. Although most equipment and media are robust there are still occasions when things can go wrong.

- Co-owners or contractors must report the loss or theft of a portable device to their line manager and to the Programme and Service Director/Digital Lead. Loss of data is potentially a Serious Untoward Incident and must be investigated immediately.

Negligence in the care of portable devices or failure to report loss or damage at the earliest opportunity may result in disciplinary action being taken against the co-owner member concerned.

All incidents relating to the security of the portable device should be reported using the organisation's incident reporting procedures.

This shall include but is not limited to:-

1. Theft/ loss of portable device
2. Disclosure of data to an unauthorised person
3. Loss/corruption of data

General Data Protection Regulations

- All portable equipment must have a machine/boot up password or user id that should be required when powered up. This is to stop unauthorised access to the information/data stored on the equipment and also to stop unauthorised persons being able to access the operating system and programmes.

- Where the equipment can receive and send data files/e-mails and attachments there will be a need to have up to date virus detection software installed.

- There must be no loading of unauthorised software. Any software on the equipment must be that which is authorised and licensed. This is loaded by the Programme and Service Director/Digital Lead and should not be tampered with by any co-owner or other person using the equipment. Any tampering of the software may be considered a disciplinary offence.

- Care should be taken if mobile computing facilities have to be used in public places/areas, meeting rooms, on the train and other unprotected areas outside of the organisation's premises. Protection should be in place to avoid the unauthorised access or disclosure of the information stored and processed by the equipment e.g. no other person should be able to access the equipment or view information on the screen.

Retention of Information

It is a requirement that when a co-owner or contractor who has a piece of portable equipment ceases working for BrisDoc that the equipment is returned to Site/Service Manager who in turn will return to the Programme and Service Director/Digital Lead, to update the Asset Register. If the equipment is to be re-assigned to another part of the organisation it will be necessary to reformat or re image the hard drive and/or delete the information that is held/stored on the equipment before it is re-assigned.

Equipment being lost or stolen

If the equipment is lost or stolen it must be reported to the Service/Site Manager or Programme and Service Director/Digital Lead immediately. This will then be documented via an incident form, investigated and then appropriate action will be taken.

Approved Usage

Where a portable device is provided by BrisDoc the portable device will be provided to each user pre-loaded with the software approved by the Digital Team. Co-owners and contractors shall not load other software onto the device, upgrade software or in any way alter software.

Co-owners must not make any hardware alterations.

BrisDoc reserves the right to audit correct usage at any time, and the individual may be held liable for illegally held software or material (e.g., in breach of copyright legislation).

Co-owners Leaving BrisDoc

Co-owners leaving the employment BrisDoc must return all their portable device(s) to their line manager. Line managers will be responsible for making sure that this is done, and that the portable device(s) is returned to the Digital Department.

Internet Connectivity and Usage

Any portable device owned by BrisDoc, which has internet connectivity, must be used in accordance with the BrisDocs internet and email policy and the information security policy.

Particular attention should be paid to the provisions relating to access to unsuitable material and activities which may compromise network security.

Wireless and Other Cordless Connectivity

Technological developments in the area of cordless connectivity (e.g. wireless connectivity, Bluetooth and infrared) have significantly increased the risks of unauthorised interception of a signal and of unauthenticated links being made to other devices. Co-owners and contractors should ensure these communication modes are switched off when not in use.

Use of USB Devices

All BrisDoc issued devices do not support the use of USB devices. If such devices are required co-owners should contact the Digital Team to provide a solution.

Disposal of Broken Devices

Devices that fail should be returned to the Programme and Service Director/Digital Lead for safe disposal.

Data Protection – Device and Media Disposal

At end-of-life Programme and Service Director/Digital Lead is responsible for ensuring that devices and media shall be disposed of or recycled in a secure fashion. Erasure of data shall be carried out. Disposal should be carried out using an approved service.

Process for Issuing Mobile Equipment

Laptops

1. Laptops will be asset tagged by the Digital Team.
2. Co-owners will be provided with guidance on how to man age and keep the laptop safe.
3. The Digital Team will setup and demonstrate the use of the Anti-Virus software to complete regular scans.
4. The Digital team will co-ordinate the reconnection of the laptops to the domain at Osprey Court monthly, to verify that antivirus software is kept up to date, no unauthorized software has been installed and that laptops are virus free.
5. Details of the asset issued to co-owners will be recorded in the Asset Log held by the Digital Team
6. Co-owners are expected to complete the monthly maintenance checks of laptop e.g., run security updates, virus updates etc. This will be checked by the Digital team.

Change Register

Date	Version	Author	Change Details
07/09/12	Vn 1.0	D Lowndes	
08/09/12	Vn 1.1	D Lowndes	Minor Amendments
21/02/14	Vn 1.2	D Lowndes	Inclusion of more prescriptive advice and control of USB devices
23/02/15	Vn 1.3	D Lowndes	Inclusion of additional guidance and process to support the remote working with laptops for both clinical and ops staff
03/03/16	V.14	D Lowndes	Addition of USB audit process
21/02/18	Vn 1.5	D Lowndes	Annual Review
21/11/2018	Vn 1.6	S Pearce/DL	DPA 1998 reference removed, GDPR reference added.
Oct-2020	Vn 1.7	DL	Version reviewed – No amendments
Nov-2023	Vn1.8	DL	Version reviewed USB references removed, si8gn off process removed as now done online. Changes references from employees to co-owners