MOBILE COMPUTING AND TELEWORKING POLICY & PROCEDURES

BADGER GROUP
Badger House
121 Glover Street
Birmingham, B9 4EY

Destroy All Previous Issues

Contents

DOCUMENT CONTROL

Document Storage

Location: P:\Ops Team\Central Policies & Procedures - Development - Word Docs\IG - IGSoc - GDPR Policies\IG-17 - Mobile and Teleworking Policy V1.8.docx

Version Control Log (Only last 3 versions, earlier versions can be found in the appropriate Archive directory for the document)

Version	Date	Author	Description of Changes
V1.6	25 July 2019	S Owen	Under review
V1.7	Oct 2019	A Savage	Reviewed, minor changes
V1.8	April 2023	A Savage	Changes to reflect new RDweb homeworker solution

Approval

Version	Name	Position	Signature	Approved Date
V1.5	IGSG	IG Steering Group		14 March 2018
V1.6	Badger Executive	Executive Team		25 July 2019
V1.7	Badger Executive	Executive Team		

Glossary

Term	Description

1 INTRODUCTION

Mobile computing is now accepted as normal working practice and includes laptops, PDA's, mobile phones and other portable devices.

There are many benefits to staff and to the care of patients using these devices. However, the portability of these devices brings a different set of risks to that of fixed systems.

Therefore, it is essential that the risk is managed properly and controls are in place to ensure patient identifiable information or commercially sensitive information is not lost or exposed inappropriately.

This document recognises the increased risk to personal information that this way of working poses and complements, but does not replace the organisation's procedures and guidelines regarding protecting patient information.

The guidelines within this document aims to support staff members in Badger who are authorised to use mobile computing equipment by ensuring they are aware of the risks of mobile computing and comply with confidentiality and security issues.

2 SCOPE

This policy and procedures covers the mobile computing equipment set out below when it has been purchased or authorised by the organisation. It does not include any equipment owned by staff. The guidelines apply to all staff including permanent, temporary, and locum members of staff.

- **Portable computer devices** - includes laptops, notebooks, tablet computers, PDA's and Smartphone's e.g. BlackBerry's, iPhones etc;
- **Removable data storage media** - 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, digital storage device (flash memory cards, USB memory sticks, portable hard drives). Essentially anything that data can be copied, saved or written to which can then be taken away and restored on another computer.

3 AUTHORISATION

Only authorised staff should have access to mobile computing equipment. Any member of staff allowing access to any unauthorised person deliberately or inadvertently may be subject to disciplinary action. Staff should **not** use their own (or unauthorised) computing equipment for organisation business.

All staff issued with mobile equipment, irrespective of the duration of the allocation, will be required to sign the assignment form attached at Appendix I. In doing so the individual confirms their agreement to comply with Badger guidelines for use of the equipment.

All allocations, transfers and removals from issue of mobile equipment will be recorded on the mobile equipment asset log that will be maintained and subject to regular review. This can be found at Appendix II.

Staff authorised and issued with mobile equipment will receive a copy of the NHS Connecting for Health, Good Practice Guide on Mobile Computing. Produced in 2008 and © Crown Copyright (Bite-sized GGP_Mobile Computing) or any replacement leaflet.

4 ENCRYPTION ON LAPTOPS

Badger staff who work from home will access Badgers domain via a remote desktop solution (RDWeb) provided by Ekco. RDWeb uses mutli factor authentication. All laptops taken off site have ESet Endpoint Antivirus

5 BACKUP

The cloud-based backup systems is designed to protect data within the organisation to ensure it is not lost and can be recovered in the event of an equipment failure, intentional destruction of data or disaster. The policy applies to all equipment and data owned operated by the organisation.

6 REMOTE WORKING

Mobile workers with authorised laptops or home computers with the necessary anti-virus software will access the Badger Network via remote desktop "RDWeb" provided by Ek.co.

Wherever possible access should be via a secure network or wi-fi connection.
User laptops have been configured allowing access to the BADGER domain via the RDweb. The steps to access are as follows:

1. *Username and password to login to the local machine*
2. *Username and password on RDWeb login which is produced by a webpage secured by "https"*
3. *2FA to access Badger domain on remote desktop*

7 ADASTRA AREMOTE

V3 Aremote is a separate Adastra software module designed to work in a semi-connected mobile environment using a portable Windows based computer. It enables mobile clinicians to receive case information from the centre whilst on the move, and to record encounter outcome information which is then automatically retrieved by the main Adastra system.

8 SECURITY

The v3 Aremote database stores minimal data. There is no case information retained once the software is shutdown. Aremote stores certain key information in its own local database, meaning that important case information is still available to the clinician even when the device is out of coverage. Main centre staff are able to flag a device as lost or stolen from the main v3 Despatch module (causing Aremote to immediately shut down and preventing it being restarted). They can also tell at a glance when each device last connected; whether the device user has received a specific case; which cases they have acknowledged as having read; and how many cases are outstanding. All communications traffic between the mobile device and the controlling centre is encrypted, using the same secure technology that banks use for their online banking services.

9 SECURITY MEASURES IN PLACE

To reduce the risk of loss and unauthorised access Badger has put the following measures in place:

- An asset control form is completed for each mobile computing device provided to a staff member; and this person is listed in the asset register as the nominated responsible owner.
- Encryption is applied to all mobile computing equipment.
- Password protected screensavers are installed on laptops;
- Anti-virus software is in use and is regularly updated. Each time the user logs into windows the software automatically updates within the background. The only requirement for the antivirus software to enable it to update is that the computer is connected to the internet so the software can download the new virus definitions to keep up to date with new threats.
- Regular backups of the remote desktop are taken and stored in the data-centre
- Disposal and re-issue of mobile computing equipment is recorded in the asset register.

10 GUIDANCE - RECOGNISING THE RISKS AND COMPLIANCE WITH RESPONSIBILITIES

You should ensure you **DO**:

- Store mobile equipment securely when not in use on and off site;
- Ensure files containing personal or confidential data are adequately protected e.g. encrypted and password protected;
- Virus check all removable media e.g. memory sticks etc prior to use;
- Obtain authorisation before you remove mobile equipment from the premises;
- Be aware that software and any data files created by you on Badger's mobile computer equipment are the property of Badger;
- Report **immediately** any stolen mobile equipment to the police and your line manager (failure to report a stolen mobile phone could result in significant charges from the organisation's telecoms provider);
- Be aware that the security of your mobile computer equipment is **your** responsibility;
- Ensure that mobile equipment is returned to Badger if you are leaving employment (A final salary deduction may be made if equipment is not returned).

You should ensure you **DO NOT**:

- Disable the virus protection software or bypass any other security measures put in place by Badger;
- Store personal information on mobile equipment unless the equipment is protected with encryption, and it is absolutely necessary to do so;
- Remove personal information off site without authorisation;
- Use mobile computer equipment outside the organisation premises without authorisation;
- Use your own mobile computer equipment for Badger business;
- Allow unauthorised personnel/friends/relatives to use mobile equipment in your charge;
- Leave mobile equipment in places where anyone can easily steal them;
- Leave mobile equipment visible in the car when traveling between locations;
- Leave mobile equipment in an unattended car;
- Leave mobile equipment unattended in a public place e.g. hotel rooms, train luggage racks; • Install unauthorised software or download software / data from the Internet;
- Delay in reporting lost or stolen equipment.

APPENDIX I – ASSIGNMENT OF MOBILE COMPUTING EQUIPMENT

ASSET CONTROL FORM		
Completion of this form is required to ensure that only authorised staff members have access to computing equipment and to ensure they sign to say they are aware of the risks of mobile computing and will comply with confidentiality and security measures.		
The following equipment has been assigned to the member of staff referred to in the **STAFF DECLARATION** at the end of this form.		
ASSET INFORMATION		
Type of asset [tick]		**Make and model**
Laptop Mobile phone Memory stick	External hard drive PDA Other [insert type]	
If the asset is a mobile phone enter number		**Serial number or for mobile - IMEI**
Date entered on asset register	**Equipment is encrypted** [circle] YES NO N/A	**Indelibly marked to indicate the property of the practice** [circle] YES NO
STAFF INFORMATION		
Allocated to [named person]**: Located at:**		

STAFF DECLARATION

I [print name]…….understand and agree to comply with the staff guidelines on using mobile computing devices and related procedures covering good information governance.

I understand that:

- It is my responsibility to report **immediately** any theft, loss, damage or misuse of the above asset.
- The equipment must be returned if I leave the employ of the organisation and that a final salary deduction may be made if equipment is not returned.
- Failure to comply with the above could lead to disciplinary action or incur financial penalties.

Signed:
Dated:

11 APPENDIX II – MOBILE COMPUTING EQUIPMENT ASSET LOG

The table below contains examples of the types of information which would be recorded in a mobile computing equipment asset log.

Asset type	Make and model	Serial number	Encryption applied	Indelibly marked YES/NO	Assigned to / date	Date decommissioned / re-issued	Action taken
EXAMPLE: Laptop			*SafeBoot*	*Yes*	~~*M. Jackson / 13/11/2009*~~ *P Jackson 12/09/2016*	*12/09/2016*	*Reassigned to P Jackson*
EXAMPLE: USB memory stick			*SafeBoot*	*Yes*	*P. Jackson*		
EXAMPLE: Mobile phone 07900 000000		*IMEI - 000000000*	*No*	*Yes*	*P. Jackson*		