REMOVABLE MEDIA ACCEPTABLE USE POLICY

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-39 - Removable Media Acceptable Use Policy V1.5.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
V1.3	July 2019	S Owen	Under review
V1.4	Dec 2019	S Owen	Minor changes
V1.5	April 2022	S Barnes	Reviewed, no changes

Approval

Version	Name	Position	Signature	Approved Date
V1.1	IGSG	IG Steering Group		09 Mar 2017
V1.2	IGSG	IG Steering Group		14 Mar 2018
V1.3	Badger Executive	Executive Team		25 July 2019

Glossary

Term	Description

1 INTRODUCTION

The aim of this policy is to explain the correct use and management of removable media on all Badger IT systems.

2 BACKGROUND

The British Standard of Information Security Management (ISO/IEC 27001) states that organisation's should implement policies for the management of removable media devices. This policy complies with regulations and standards published by the Department of Health.

The Information Security Management: NHS Code of Practice published by the Department of Health makes reference to the use of information assets such as digital media and the need for a robust information security framework to comply with legal requirements.

3 SCOPE OF POLICY

This policy applies to all Badger staff (including substantive, temporary, student, honorary staff etc) and all other third party users on Badgers premises, or at any other location.

A breach or refusal to comply with this policy is a disciplinary offence, which may lead to disciplinary action, and in the appropriate circumstances, dismissal without notice. Any such disciplinary action is to be taken in accordance with the current Badger disciplinary policy.

You must conduct yourself, at all times, in a trustworthy and appropriate manner so as not to discredit or harm Badger, or its staff, and in accordance with the spirit of this policy.

4 WHAT IS REMOVABLE MEDIA?

Removable media can be defined as any portable device that can be used to store and move information. Media devices can come in various formats, including:

- Universal Serial Bus (USB) memory sticks (also known as flash disks or flash drives)
- External hard drives
- Compact disks (CD)
- Digital Versatile Disks (DVD)
- USB Hard Disk Drives
- Secure Digital Cards
- MP3 / MP4 players i.e. iPODs or any other brands
- Mobile phones and digital cameras
- Dictation Devices
- Tablet Devices

(This list is not exhaustive please contact the IT Department to clarify the use of any other media devices not listed above)

Essentially, anything you can copy, save and/or write information to which can then be taken away and transferred

or read on another computer.

5 OBJECTIVES

The objective of this policy is to:

- Ensure staff are aware that they cannot use removable media devices unless they have been either provided or authorised by Badger.
- Ensure users of removable media devices understand their responsibilities regarding appropriate and proper use.
- Identify the organisational responsibilities for supplying removable media devices.

6 RISKS

- The risk of uncontrolled access to, and copying of, information is heightened, as most forms of removable media require no form of authentication, password protection, or configuration to install or use. They can make use of 'plug and play' technologies and generally do not require any administer privileges to install.

- The risk of unauthorised disclosure of personally identifiable information or other special category data along with the obvious potential for legal action or public embarrassment to the Badger if an item of removable media fell into the wrong hands.

- The risk that removable media can be used to inadvertently transfer malicious software onto other Badger systems along with, or as part of authorised data.

- The nature and tangible size of removal media is such that they are also prone to accidental loss and / or theft

.

- The risk that the version control of a document may be lost if only stored on removal media.

- The loss of information if an item of removable media became damaged or corrupted.

7 USER RESPONSIBILITIES

7.1 What you can do:

- Only use Badger provided encrypted removable media devices provided there is a legitimate business reason and with the prior approval of a member of Badger Exec..

- Ensure personal responsibility and security for any Badger provided removable media device in your care.

- Return any removable digital media devices no longer required to the IT department to be either cleared and reused or physically destroyed.

7.2 What you can't do:

- Connect any personal device to the Badger network, this includes connecting mobile phones to a USB port to charge a battery.

- Remove the USB blocker panels.

- Use any removable media devices unless you are specifically authorised to do from the Badger Exec and IT Department.

- Use Badger provided removable media devices for the transfer or storage of person identifiable data in bulk form unless the device has been encrypted.

- Use removable media for the bulk transfer of data off site without the consent of Badgers Caldicott Guardian and IT Department.

- Use any personally removable media devices without Badger standard encryption in place and without the authorisation of a member of Badger Exec and IT Department.

- Use personally provided removable media for the transfer or storage of personally identifiable information or special category data.

- Use Badger provided removable media devices as a permanent or indefinite storage mechanism. Data must be transferred, as soon as possible to a secure networked drive and removed from any Badger provided device.

- Use removable media devices to introduce viruses onto the Badger network.

- Store portable devices in an insecure manner when not in use either on or off site.

- Use Badger provided removable media devices for any type of commercial or profit-making nature, or for any other form of personal financial gain. Or any use that conflicts with an employee's obligations to their employer. Or any use considered being against Badgers rules, regulations, policies and procedures in particular this policy.

7.3 Additional Requirements:

- Whilst in transit all removable media should be secured discretely not in public view where it can attract attention.

- All removable media is to be clearly labelled to identify its ownership by Badger.

- All removable media should be stored in the environment conditions as specified by the manufacturer's recommendations.

8 CLASSES OF INFORMATION

The correct use of removable media must be based upon the sensitivity of the material to be secured on it. For the purpose of this policy, information is split into two separate categories: -

- Confidential Information
- Unclassified Information

8.1 Definition of Confidential Information

For the purpose of this policy, confidential information includes:

- Personally identifiable information 9patinet and/or staff)
- Special category data
- Disciplinary, grievance or other investigation reports (SUIs) and associated documents
- Corporate or contractually sensitive information
- Time embargoed information

The decision as to whether or not information falls into this category rests with the author or owner of any document. If a member of staff is unsure whether a document should be treated as confidential or not, it must be treated as confidential.

8.2 Definition of Unclassified Information

For the purpose of this policy, unclassified information includes those documents that have no classification requirement and should NOT include confidential or sensitive information.

For example, any documentation already within the public domain i.e. Terms of reference, minutes from meetings, policies, published documents on the intranet and extranet.

9 CONNECTING REMOVABLE MEDIA

This paragraph introduces guidance for connecting removable media to the Badger network and to computers owned by other organisation and companies.

9.1 Using Removable Media on non-Badger computers

Removable media owned by Badger may be connected to non-Badger owned computers where a legitimate professional reason exists and the consent of the host has been given. If a legitimate professional relationship does not exist, the removable media is not to be connected.

9.2 Connecting Third Party Removable Media to Badger computers

Removable media owned by other companies or individuals may be connected to Badger owned computers but only where a legitimate professional reason exists. It a legitimate professional reason does not exist, the removable media is not to be connected.

10 THE PROCUREMENT AND AVAILABILITY OF REMOVABLE MEDIA

The procurement of removable media is only to be carried out by the IT Department. Only approved USB memory sticks can be used / purchased.

The disposal of removable media devices that may hold personal identifiable or highly sensitive information must be referred to the IT Department.

In liaison with the IT Department removable media devices in need of repair should be returned to the IT Department. It is the responsibility of the IT Department to ensure that all sensitive information is deleted from the device prior to disposal.

Software and data held on removable mobile devices is subject to the same audit procedures as all other Badger computer systems. This applies to any data stored on removable data storage media.

11 REPORTING THE LOSS OF REMOVABLE MEDIA

All members of staff must report the loss, whether stolen or mislaid, of any item of removable media. This reporting must be made to:

- Line Manager
- IT Department
- Information Governance Lead

This reporting must be carried out as soon as possible after the loss is identified.

11.1 Legislation / Statutory Requirements

Human Rights Act 1998
Rights and freedoms protected under the European Convention on Human Rights.

Equality Act 2010
Provisions relating to Human Rights and discrimination on grounds of race, religion or belief sexual orientation; sex; amends the Disability Discrimination Act 1995.

- Data Protection Act 2018
- Computer Use Act 1990
- Copyright, Design and Patents Act
- Electronic Communication Act
- Common Law Duty of Confidentiality
- Caldicott Principles