Transport for Greater Manchester

Transport for Greater Manchester Policy

IS Removable Media Policy

Warning:

Printed copies of this document are uncontrolled

Check issue number on Intranet before using.

Date Prepared:	31st March 2019	Document Reference no.	IS Removable Media Policy Ref No. 022
Version No.	8.0	Prepared by:	Catherine Burke
Equality Impact Assessment	Validation of Initial Screening Equality Officer: Muhammad Karim		Full Impact Assessment completed: YES **Validated by Equality Officer signature:** **Date:**
Authorisation Level required:	Executive Group/Director		Staff Applicable to: All Staff
Authorised by: Date:	Head of IS (Malcolm Lowe) 31st March 2019		Implementation date: 31st March 2019 Annual review date: 31st January 2020

1 Policy Aims

Removable media is a well-known source of malware infections and has been directly tied to the loss of sensitive information in many organisations.

This policy describes Removable Media policy for;

External Devices: Any device that can be connected to a PC or mobile device, using USB or other connections. This includes pen drives, USB sticks, external hard drives, cameras, camcorders, phones, blackberry's, IPods, MP3 and other music players.

Portable Media: CD's, DVD's, floppy disks, CF or SD cards and similar portable media.

2 Policy Scope

To minimise the risk of loss or exposure of sensitive information maintained by **TfGM** and to reduce the risk of acquiring malware infections on computers operated by **TfGM**.

This policy covers all computers and servers operating in **TfGM**.

3 Policy Delivery

This policy will be delivered to all staff by internal communication and will be situated on the **TfGM** Intranet.

4 Accountability

- **Responsible to the Board:** Head of IS
- **Compliance:** IS Operations
- **Awareness:** IS Department

5 Policy Monitoring/ Compliance

a) This policy will be enforced by the Executive.

b) Information including logon dates, times, usage duration and device identity will be logged and maybe used for monitoring purposes, and disciplinary proceedings.

c) Should a breach or violation of this policy be identified, it may result in disciplinary action in accordance with **TfGM** disciplinary policy.

d) In extreme circumstances Audit & Assurance may access equipment or information to help support investigations.

6 Policy

a) This policy aims to minimise the risk of loss or exposure of sensitive information maintained by **TfGM** and reduce the risk of acquiring malware infections on computers operated by **TfGM**.

b) **TfGM** staff may only use **TfGM** removable media in their work computers.

c) **TfGM** removable media may not be connected to or used in computers that are not owned or leased by the **TfGM** without explicit permission of the **TfGM** Head of IS or IS Director.

d) Sensitive information should be stored on removable media only when required in the performance of your assigned duties.

e) Where any information is stored on removable media, it must be encrypted in accordance with the TfGM Acceptable Encryption Policy.

6.1 Staff MUST NOT

- Attach personal or non-**TfGM** owned hardware or removable devices to **TfGM's** corporate network or PCs/Laptops.
- Charge any personal equipment using USB ports or PC's or Laptops – if devices are infected with viruses, they can still infect the network even when just charging.
- Run any portable applications from USB sticks unless they are licensed to **TfGM** and authorised by IS.
- Attach any **TfGM** owned media or devices to personal or external third party computer equipment.
- Transport any sensitive or personal data on removable media.

6.2 Best Practice Guidelines

- If there is a requirement to send data to third parties, using removable media, IS should be consulted for advice on encryption and safe transit.
- If there is an essential business need for the use of any external media or devices, an IS Service request must be submitted to IS. Where authorised appropriate equipment will be issued along with guidance on how to secure ad check for viruses.
- Where essential business critical data is received from third parties on removable media, users should bring the media to Serviceline to be virus checked on a computer without network access, with up to date virus signatures, prior to use.
- Staff must advise any visitors in their charge as to removable media policy and supervise at all times to ensure that the policy is not breached.
- When in transit between work and home or off site destination, unencrypted removable media should not be transported in the same case as a laptop case in case of loss or theft.

7 Enforcement

This policy will be enforced by the Executive and violations may results in disciplinary action in accordance with TfGM disciplinary policy.

8 Definitions

Removable Media: Device or media that is readable and/or writeable by the end user and is able to be moved from computer to computer without modification to the computer. This includes flash memory devices such as thumb drives, cameras, MP3 players and PDAs; removable hard drives
(including hard drive-based MP3 players); optical disks such as CD and DVD disks; and any commercial music and software disks not provided by TFGM.

Encryption: A procedure used to convert data from its original form to a format that is unreadable and/or unusable to anyone without the tools/information needed to reverse the encryption process.

Sensitive Information: Information which, if made available to unauthorised persons, may adversely affect TFGM and its programs, or participants served by its programs.

Malware: Software of malicious intent/impact such as viruses, worms, and Spyware.

- *Change control record: complete each time there is a change*

Policy/Procedure:				
Version	Change	Reason for change	Date	Name
3.0	Date and version	Annual Review	06/03/2014	C Burke
4.0	Date and Version	Annual Review	30/04/2015	C Burke
5.0	Date and Version	Annual Review	31/03/2016	C Burke
6.0	Date and Version	Annual Review, new Head of IS	31/03/2017	C Burke
7.0	Date and Version	Annual Review	31/03/2018	C Styler
8.0	Date and Version	Annual Review	31/03/2019	C Styler