Transport for Greater Manchester

Transport for Greater Manchester Policy

IS Mobile Device Usage 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 Mobile Device Usage Policy Ref No. 016
Version No.	7.0	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

Table of Contents

1 Policy Aims

The purpose of this policy is to specify **TfGM** standards for the use and security of mobile devices.

2 Policy Scope

TfGM utilises Mobile devices to enable the workforce to work in more flexible ways, therefore special consideration must be given to the security of mobile devices especially when sensitive data is stored on them.

This policy applies to all types of mobile devices that are capable of coming into contact with **TfGM** data, including, but not limited to, laptops, notebooks, PDAs, smart phones, mobile phones and USB drives irrelevant of the owner of the devices.

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 Staff
- Awareness: All

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 Physical Security

A mobile device is more susceptible to loss or theft than a non-mobile device. Users must carefully consider the physical security of mobile devices and take appropriate protective measures, including the following:

a) Laptop locks and cables must be used to secure laptops when left in the office or other fixed locations. Alternatively a laptop can be locked away in a secure drawer or cabinet.
b) Mobile devices should be kept out of sight when not in use.
c) Care should be given when using or transporting mobile devices in busy areas.
d) Mobile devices must not be stored in cars. If the situation leaves no other viable alternatives, the device must be stored in the car boot, with the interior boot release locked; or in a lockable compartment such as a glove box.

For all mobile devices connected to the **TfGM** network and where practical a remote wipe/remote delete technology must be implemented.

7 Connecting to the TfGM Network

All mobile devices that are connected to the **TFGM** network must be authorised by the Head of IS, any unauthorised devices must be explicitly denied access.

8 Data Security

8.1 TfGM Owned Mobile Devices

If a **TfGM** mobile device is lost or stolen, the data security controls that were implemented on the device are the last line of defence for protecting **TfGM** data. The following sections specify **TfGM** requirements for data security:-

8.2 Laptops/Devices

a) All laptops must have whole disk encryption and as a minimum require a username and password for login.

b) Portable computing devices, such as laptops/surfaces are provided to assist flexible working. Staff issued with this equipment are to ensure that it is used as portable and not left in 2PP, unless exceptional circumstances exist. In the event of a major incident portable devices will be reallocated to priority services involved in recovery activities.

8.3 Smart Phones and Mobile Devices

a) All devices that are connected to the IS infrastructure must be protected by a password of at least 4 characters and automatically locks after 10 minutes of inactivity.

b) The maximum number of retries for entering a password is 4, after 4 unsuccessful logon attempts the devices must be reset to the factory default settings removing all **TfGM** related information and require the IS Department to authorise the device for reconnection to the **TfGM** domain.

c) The password must be changed every 90 days as a minimum. All **TfGM** devices that store sensitive information are capable of being remotely wiped to ensure any **TfGM** related data contained on them is protected from unauthorised access.

8.4 Mobile Storage Media

a) Only IS supplied and approved USB drives, flash drives, memory sticks or other personal data storage media can be used to store business information.

b) Storage of **TfGM** data on such devices is not allowed if the information is confidential in any way, unless the device is encrypted.

c) Non-sensitive information can be stored on these devices without encryption if it is required for business use.

8.5 Portable Media Players

TfGM data cannot be stored on personal media players.

8.6 Other Mobile Devices

Unless specifically addressed by this policy, storing **TfGM** data on other mobile devices, or connecting such devices to **TfGM** systems, is expressly prohibited.

9 Personal Mobile Devices (not owned by TfGM)

Many mobile phones or other devices, often called smartphones, provide the capability to send and receive email. This can present a number of security and data protection issues, since sensitive **TfGM** data could be stored on the phone.

If an employee requires access to **TfGM** via the use of their own mobile device, then the following sections specify **TfGM** requirements for data security:-

9.1 Private Mobile

Users private mobile devices can be connected to **TFGM's** e-mail system provided that:

- Access has been signed off by the appropriate Director on the 'Mobile Communications Form'.
- The device is PIN protected.
- If the device is lost the loss will be reported to **TFGM's** IS Department who will then 'wipe' the device, this will remove ALL data from the device including the users own personal data.
- **TfGM** will not provide support for non **TfGM** supplied devices.

9.2 Outlook Web Access

a. Access to **TfGM** email from a non-**TfGM** device must only be made via a secure Outlook Web Access session. This method enables the viewing and sending of **TfGM** emails in a safe and secure manner since data is not downloaded to the device but viewed in an encrypted browser session.

b. If you are accessing emails in this manner on a non-**TfGM** device, then there is a mandatory requirement for you to change you system login password immediately should the personal mobile device become lost or stolen.

c. It is prohibited to download **TfGM** emails to a personal mobile phone for data protection and security reasons.

d. Note that this section does not apply if **TfGM** provides the phone and mobile email access as part of its remote access plan. In this case, permission is implied.

9.3 TfGM Wireless

The use of the **TfGM** Wireless is only for business purposes and should not be used for non-business use or as a means to by-pass the Content filter.

All usage is monitored by the IS Department.

10 Connecting to Unsecured Networks

Users must not connect to any outside network without a secure, up-to-date software firewall configured on the mobile computer.

Examples of unsecured networks would typically, but not always, relate to Internet access, such as access provided from a home network, access provided by a hotel, an open or for-pay wireless hotspot, a convention network, or any other network not under direct control of **TfGM**.

11 Audits

This document is part of the **TfGM's** cohesive set of IS policies. Other policies may apply to the topics covered in this document and as such the applicable policies should be reviewed as needed.

12 Enforcement

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

13 Definitions

Encryption: The process of encoding data with an algorithm so that it is unintelligible without the key. Used to protect data during transmission or while stored.

Mobile Devices: A portable device that can be used for certain applications and data storage. Examples are PDAs or Smartphones.

Mobile Storage Media: A data storage device that utilises flash memory to store data. Often called a USB drive, flash drive, or thumb drive.

Password: A sequence of characters that is used to authenticate a user to a file, computer, or network. Also known as a passphrase or passcode.

PDA: Stands for Personal Digital Assistant. A portable device that stores and organises personal information, such as contact information, calendar, and notes.

Portable Media Player: A mobile entertainment device used to play audio and video files. Examples are mp3 players and video players.

Smartphone: A mobile telephone that offers additional applications, such as PDA functions and email.

- *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

6.0	Date and Version	Annual Review	30/03/2018	C. Styler
7.0	8.2(b) Laptops/Devices	Flexible working/portable devices	21/11/2018	C.Burke
8.0	Date and Version	Annual Review	30/03/2019	C. Styler