Transport for Greater Manchester

Transport for Greater Manchester Policy

IS Wireless Access 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 Wireless Access Policy Ref No. 031
Version No.	6.0	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 state the standards for wireless access to **TfGM's** network. Wireless access can be done securely if certain steps are taken to mitigate known risks. This policy outlines the steps that must be taken to secure the wireless infrastructure.

2 Policy Scope

Wireless communication really is an increasingly important role in the workplace. In the past, wireless access was the exception; it has now become the norm in many companies. However, while wireless access can increase mobility and productivity of users, it can also introduce security risks to the network.

This policy covers anyone who accesses the network via a wireless connection. The policy further covers the wireless infrastructure of the network, including access points, routers, wireless network interface cards, and anything else capable of transmitting or receiving a wireless signal.

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:** All Staff

5 Policy Monitoring/ Compliance

All wireless connection information, including dates, times, duration and device identity may be logged for monitoring purposes and should a breach of policy be identified, may be used in disciplinary proceedings.

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) Unsecured Wireless Internet is provided for the use of visitors only, at their own risk.

b) This unsecured connection is not protected from internet attacks by any security systems and **TfGM** will not accept responsibility for any damage to visitor's equipment incurred from malware or other causes, as a result of using this connection.

c) It must not be used under any circumstances to bypass the Websense internet filtering security. In the event that a breach of these guidelines is discovered then disciplinary action, up to and including dismissal, may be taken.

d) **TfGM** reserves the right to withdraw access to the Guest Wireless Internet facility at any time.

e) An individual time limited password may be obtained for visitors by contacting Serviceline. This password must not be divulged to any other guest or **TfGM** staff.

f) It is the responsibility of the member of staff obtaining the password on behalf of the visitor to ensure that it is used in accordance with the **TfGM** Internet Usage Policy and that the visitor does not breach those guidelines causing the reputation of **TfGM** to be brought into disrepute.

6.1 Physical Guidelines

Unless a directional antenna is used, a wireless access point typically broadcasts its signal in all directions. For this reason, access points must be located central to the office space rather than along exterior walls. If it is possible with the technology in use, signal broadcast strength must be reduced to only what is necessary to cover the office space.

Directional antennas should be considered in order to focus the signal to areas where it is needed.

Physical security of access points must be considered. Access points must not be placed in public or easily accessed areas. Access points must be placed in non-obvious locations (i.e., above ceiling tiles) so that they cannot be seen or accessed without difficulty.

6.2 Configuration and Installation

The following guidelines apply to the configuration and installation of wireless networks:

6.2.1 Security Configuration

1. The Service Set Identifier (SSID) of the access point must be changed from the factory default. The SSID must be changed to something completely nondescript. Specifically, the SSID must not identify TfGM, the location of the access point, or anything else that may allow a third party to associate the access point's signal to TfGM.
2. The SSID must not be broadcast. This adds a layer of security by requiring wireless users to know the SSID in order to connect to the network.
3. The wireless access point must utilise Mac address filtering so that only known wireless NICs are able to connect to the wireless network.
4. The wireless access point must not connect to the trusted network without a firewall or other form of access control separating the two networks.
5. Encryption must be used to secure wireless communications. The strongest available algorithm must be used (i.e., WPA rather than WEP). Encryption keys must be changed and redistributed quarterly.
6. Administrative access to wireless access points must utilise strong passwords.
7. All logging features must be enabled on the wireless access points.
8. Wireless networking should require users to authenticate against a centralised server. These connections should be logged, with the IS Department reviewing the log regularly for unusual or unauthorised connections.
9. Wireless LAN management software should be used to enforce wireless security policies. The software must have the capability to detect rogue access points.
10. TfGM users accessing the wireless network must be provided with a personal software firewall to secure their computers.

6.2.2 Installation

The following must be adhered to for wireless installations:

1. Software and/or firmware on the wireless access points and wireless network interface cards (NICs) must be updated prior to deployment.
2. Wireless networking must not be deployed in a manner that will circumvent the security controls.
3. Wireless devices must be installed only by the IS Department.
4. Channels used by wireless devices must be evaluated to ensure that they do not interfere with TfGM equipment.

7 Accessing Confidential Data

Wireless access to confidential data is permitted as long as the access is consistent with this and other policies that apply to confidential data.

8 Definitions

Mac Address: Short for Media Access Control Address. The unique hardware address of a network interface card (wireless or wired). Used for identification purposes when connecting to a computer network.

SSID: Stands for Service Set Identifier. The name that uniquely identifies a wireless network.

WEP: Stands for Wired Equivalency Privacy. A security protocol for wireless networks that encrypts communications between the computer and the wireless access point. WEP can be cryptographically broken with relative ease.

WiFi: Short for Wireless Fidelity. Refers to networking protocols that are broadcast wirelessly using the 802.11 family of standards.

Wireless Access Point: A central device that broadcasts a wireless signal and allows for user connections. A wireless access point typically connects to a wired network.

Wireless NIC: A Network Interface Card (NIC) that connects to wireless, rather than wired, networks.

WPA: Stands for WiFi Protected Access. A security protocol for wireless networks that encrypts communications between the computer and the wireless access point. Newer and considered more secure than WEP.

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

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