Transport for Greater Manchester

Transport for Greater Manchester Policy

IS Acceptable Use 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 Acceptable Use Policy 001
Version No.	8.0	Prepared by:	Catherine Burke
Equality Impact Assessment	Validation of Initial Screening Equality Officer: Muhammad Karim **Date:**		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: January 31st 2020

Table of Contents

1 Policy Aims

a) **TfGM** is committed to protecting its employees, partners and company from illegal or damaging actions by individuals.

b) This document describes what acceptable usage on **TfGM's** Information Systems is.

c) Since inappropriate use of **TfGM's** IS Systems exposes **TfGM** to unacceptable risk, it is important to specify exactly what is permitted and what is not permitted.

d) **TfGM** E-mail policy is published on the **TfGM** Intranet.

2 Review and Update of the Policy Statement

a) The Policy Statement and associated company Policies are reviewed at least annually by **TfGM's IS Team** to ensure:

- Appropriate use of IS Systems resources including, but not limited to, computer systems, email, internet and network access.

b) The **IS Team** will undertake the review of this policy statement and associated company Policies.

3 Purpose

a) **TfGM** is committed to protecting its employees, partners and the company from illegal or damaging actions by individuals, either knowingly or unknowingly.

b) These rules are in place to protect both employees and **TfGM**, as inappropriate use exposes **TfGM** to risks including virus attacks, and potential compromise of network systems and services.

4 Scope

a) This policy applies to users wishing to access **TfGM**'s infrastructure resources, (i.e. Email, Skype for Business (SfB), Internet, tablets, laptops, ipads etc) and applies to employees, contractors, consultants, and other workers at **TfGM**, including all personnel affiliated with third parties.

b) This policy applies to all associated equipment that is owned or leased by **TfGM**.

5 Policy Delivery

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

6 Accountability

i) **Responsible to the Board**: Head of IS

ii) **Compliance**: All Staff

iii) **Awareness:** All Staff

7 Enforcement / 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.

8 Policy

8.1 General Use and Ownership

a) Whilst **TfGM** shall ensure that all necessary and prudent measures are taken to secure its infrastructure from attack, it is the user's individual responsibility to maintain the security of his or her account by not writing down or sharing their password.

b) If a user knows or suspects that their account password has been compromised, they must immediately inform Serviceline of their concerns and carry out the instructions issued to them by the IS Team.

c) IS Systems are the property of **TfGM** and are only to be used for business purposes, serving the interests of the company, clients and customers in the course of normal operations.

d) The **IS Team** recommends that any information considered to be sensitive or vulnerable is encrypted. For guidelines on information classification, see Information Classification Policy.

e) For security and network maintenance purposes, authorised individuals within **TfGM** may monitor equipment, systems and network traffic at any time.

f) 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.

8.2 Internet Use

a) **TfGM** recognises that the Internet can be a tool that is useful for both personal and professional purposes.

- Personal usage of **TfGM** computer systems to access the Internet is permitted during lunch breaks, and before/after business hours (within the permitted quota) as long as such usage does not

contravene this or other IS policies and does not have a detrimental effect on **TfGM** or on the employee's job performance.

b) **TfGM** reserves the right to monitor Internet use.

c) Access to internet sites, which contain pornographic, exploitative, offensive, discriminatory or criminal content, will result in disciplinary action. If illegal content has been accessed, the Police will be informed.

d) **TfGM** have outlined the restrictions on use of e-mail, Skype for Business (SFB) and internet services within the **TfGM** E-mail Policy.

8.3 Email Use & Skype for Business (SfB) Use

a) Personal usage of the **TfGM** email & SfB system is permitted as long as such usage does not negatively impact:

- **TfGM's** network performance.
- Individuals performance
- **TfGM's** reputation

a) **TfGM** reserves the right to monitor and archive emails.

b) **TfGM** may filter email & SfB content, and block any email that is deemed inappropriate.

8.4 Unacceptable Use

a) The following actions shall constitute unacceptable use of the **TfGM** network. The list is not exhaustive, but is included to provide a reference for types of activities that are deemed to be unacceptable. Users **must not** use the **TfGM** network and/or systems to:

- Engage in activity that is illegal under local, UK, or international law.
- Engage in any activities that may cause embarrassment, loss of reputation, or other harm to **TfGM**.
- Disseminate defamatory, discriminatory, vilifying, sexist, racist, abusive, rude, insulting, threatening, obscene or otherwise inappropriate messages or media.
- Perform any of the following; port scanning, security scanning, network sniffing, keystroke logging or other IS information gathering techniques when not part of an individual's job function.
- Install or distribute unlicensed or 'pirated' software.
- Reveal system or network passwords to others, including **TfGM** employees, family, friends, or other members of the household when working from home or remote locations. This could lead to a potential compromise of security and disciplinary action.
- Extract data or share data with third parties, unless in accordance with their **TfGM** duties.

If any staff member is concerned whether an action they are about to undertake contravenes this policy than they must consult Serviceline undertaking the actions.

8.5 Blogging and Social Networking

a) Blogging and social networking by **TfGM** employees is subject to the terms of this policy, whether performed from the **TfGM** network or from personal systems.

b) Personal blogging and social networking is not allowed from the **TfGM** computer network.

c) Under no circumstances, including blogs or sites published from personal or public systems, should **TfGM** be identified, **TfGM** business matters are discussed, or material detrimental to **TfGM** be published.

d) Individuals must not identify themselves as an employee of **TfGM** on any blog or social networking site.

e) Individuals assume all risks associated with blogging and/or social networking.

f) The only exceptions to this policy are blogs, posts or website content authorised and approved by the Communications and Customer Services Director or Public Relations Manager in writing.

8.6 Copyright Infringement

a) **TfGM** computer systems and networks must not be used to download, upload, or otherwise handle illegal and/or authorised copyrighted content. Any of the following activities constitute violations of acceptable use, if done without permission of the copyright owner:

- Copying and sharing images, music, movies, or other copyrighted material using P2P file sharing or unlicensed CD's and DVD's.
- Posting or plagiarising copyrighted material.
- Downloading copyrighted files which the employee has not already legally procured.

Note: This list is not meant to be exhaustive, copyright law applies to a wide variety of works and applies to much more than is listed above.

8.7 Monitoring and Privacy

a) Individuals should not expect privacy when using the **TfGM** network or resources. Such use may include but is not limited to; transmission and storage of files, data, and messages. **TfGM** reserves the right to monitor any and all use of the IS systems, network and services.

b) To ensure compliance with **TfGM** policies, monitoring may include the interception and review of any emails, or other

messages sent or received, inspection of data stored on personal file directories, hard disks and removable media.

8.8 Non TfGM Equipment

a) Only **TfGM** equipment is expressly allowed to be physically connected to the IS network via a network cable on the IS network.

b) BYOD (Bring Your Own Device) mobiles and personal devices are allowed to connect via the guest wireless network, but accessing subject to adherence to the Internet Use Policy.

8.9 Reporting of Security Incident

If a security incident or breach of any security policies is discovered or suspected, the user must immediately notify his or her supervisor and/or follow any applicable guidelines as detailed in **TfGM** IS Incident Response Policy. Examples of incidents that require notification include:

- Suspected compromise of login credentials (username, password, etc).
- Suspected virus/malware/trojan infection.
- Loss or theft if any device that contains company information.
- Loss or theft of ID badge or key card.
- Any attempt by any person to obtain a user's password over the telephone or by email.
- Any other suspicious event that may impact **TfGM** information security.

Users must treat a suspected security incident as confidential information, and report the incident to their supervisor and the IS Department. Users must not withhold information relating to a security incident or interfere with an investigation.

9 Definitions & References

9.1 Definitions

Bandwidth Usage: amount of data transmitted and received by a particular computer or user. The more data exchange that occurs, the higher the potential to clog the network.

Blogging: The process of writing or updating a “blog”, which is an online, user-created journal (short for “web log”).

Copy Infringement: The use of works under copyright, infringing the copy rights holder’s exclusive rights, such as the right to reproduce, distribute, display or perform the copyrighted work, or to make derivative works without permission from the copyright holder, which is typically a publisher or other business representing or assigned by the workers creation.

Encryption: Encryption refers to algorithmic schemes that encode onto plain text non-readable form or cypher text, providing privacy. The receiver of the encrypted text uses a "key" to decrypt the message, returning it to its original plain text form. The key is the trigger mechanism to the algorithm.

Keystroke Logging: Keystroke logging, also known as key logging, is the practice of recording the data entered by a computer user during the use of a computer’s keyboard.

Malware: short for **malicious software**, is software used or programmed by attackers to disrupt computer operation, gather sensitive information, or gain access to private computer systems

Network Sniffing: is scanning the communication on a network for either diagnostic or malicious reasons. Benign cases are also known as network monitoring malicious cases are more likely called packet sniffing.

Pen Drive: A pen drive is a portable Universal Serial Bus (USB) flash memory device for storing and transferring audio, video, and data files from a computer.

Personal Data: Personal data is anything which identifies you as an individual, either on its own or by reference to other information.

Pirated Software: Pirated software is software which has been duplicated and distributed without authorization. A number of activities could be considered software piracy, with the classic example being someone who makes multiple copies of a program and sells the copies

Plagiarising: The act of appropriating the literary composition of another author, or excerpts, ideas, or passages therefrom, and passing the material off as one's own creation.

Port Scanning: A **port scanner** is a software application designed to probe a server or host for open ports. This is often used by administrators to verify security policies of their networks and by attackers to identify running services on a host with the view to compromise it.

P2P File Sharing: A distributed network of users who share files by directly connecting to the users computers over the internet rather than through a central server.

Remote Desktop Access: Remote control software that allows users to connect to, interact with, and control a computer over the Internet just as if they were sitting in front of that computer.

Removable Electronic Media: Removable media is a method of storing computer data via usually magnetic or optical means. This data is contained on portable storage devices that are not physically attached to a computer in a permanent fashion such as the factory-installed hard drive is meant to be.

Security Scanning: An anti-virus software that detects viruses, trojans and malware.

Social Networking: Social networking is the grouping of individuals into specific groups, like small rural communities or a neighbourhood subdivision, if you will. Although social networking is possible in person, especially in the workplace, universities, and high schools, it is most popular online.

Trogan: A Trojan is a program that may appear to be legitimate, but in fact does something malicious. Trojans are often used to gain backdoor access - that is to say remote, surreptitious access, to a user's system

Virus: A **computer virus** is a type of malware that, when executed, replicates by inserting copies of itself (possibly modified) into other computer files, data files, or the boot sector of the hard drive; when this replication succeeds, the affected areas are then said to be "infected".

Wireless communication is the transfer of information between two or more points that are not connected by an electrical conductor.

Policy: P06 – IS Acceptable Use Policy				
Version	**Change**	**Reason for change**	**Date**	**Name**
2.0	Ipads Added	Review	31/10/2013	C. Burke
2.0	Pen Encryption Change	Review	31/10/2013	C. Burke
3.0	Date & Version	Annual Review	31/03/2014	C. Burke
4.0	Date & Version	Annual Review	30/04/2015	C. Burke
5.0	Date & Version	Annual Review	31/03/2016	C Burke
5.1	SfB added	New rollout for SfB	07/07/2016	C. Burke
6.0	Date & Version	Annual review, new Head of IS	31/03/2017	C. Burke
6.0	Date & Version	Annual Review	31/03/2018	C Styler
7.0	8.1(i) General Use	Flexible working/Mobile Devices	21/11/2018	C. Burke
8.0	IS Operation manager removed	Annual review	29/03/2019	C.Styler