Transport for Greater Manchester

Transport for Greater Manchester Policy

IS Virus and Anti-Virus 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 Virus & Anti-Virus Policy Ref No. 029
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:	Head of IS (Malcolm Lowe)		Implementation date: 31st March 2019
Date:	31st March 2019		Annual review date: 31st January 2020

Table of Contents

1 Policy Aims

This policy is an internal IS Policy which defines anti-virus policy on every computer including how often a virus is done, how often updates are done, what programs will be used to detect, prevent, and remove software malware.

It defines what types of files attachments are blocked at the mail server and what anti-virus program will be run on the mail server.

This document describes prevention of viruses and other malware that relate to;

Desktops & Servers: All accessible PC’s, Network drives

Telephony: Mobile Phones, PDA’s, Smartphone’s, Blackberrys, iphones

Wireless Computing: Laptops, Notebooks, Tablets

Removable Media: Pen Drives, Camera’s, Ipods, USB Drives

Externally Facing Programs: Email, Internet, FTP

2 Policy Scope

This policy is designed to protect the organisational resources against intrusion by viruses and other malware.

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) All **TfGM** computers and mobile devices must have **TfGM's** standard, supported anti-virus software (Trend antivirus currently) installed and scheduled to run at regular intervals.

b) In addition, the anti-virus software and the virus pattern files must be kept up-to-date. Virus-infected computers must be removed from the network until they are verified as virus-free.

c) IS are responsible for creating procedures that ensure anti-virus software is run at regular intervals, and computers are verified as virus-free.

d) Any activities with the intention to create and/or distribute malicious programs into **TfGM's** networks (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.) are prohibited, in accordance with the Computer Misuse Act.

e) Refer to **TfGM's** Anti-Virus recommended processes to help prevent virus problems.

Noted exceptions: Machines with operating systems other than those based on Microsoft products may be excepted at the current time.

6.1 Anti-Virus Recommended Processes

- Only run the corporate standard, supported anti-virus software. Make sure you are familiar with the antivirus icon in the bottom right hand side of your computer screen. If your antivirus icon is missing or alters from the normal blue icon please inform Serviceline immediately as you will be no longer fully protected. If you get a pop up from the antivirus software requesting you to reboot to complete the removal of a virus or to update components, please do so immediately.

- Do not click on links in emails that you are not expecting, they are likely to lead to an untrustworthy website, which may either infect your PC with malware or attempt to steal your identity.
- NEVER open any files or macros attached to an email from an unknown, suspicious or untrustworthy source. Delete these attachments immediately, then "double delete" them by emptying your Deleted Items folder.
- Delete spam, chain, and other junk email without forwarding, as in **TfGM's** Electronic Messaging Policy.
- Keep internet usage to a minimum. Only use the internet if it is absolutely necessary for business critical work. Be aware that 'reputable' sites are more likely to be targeted with malware as they are guaranteed to be visited.
- Never download files from unknown or suspicious sources, they are likely to have malware attached to them.
- Avoid direct disk sharing with read/write access unless there is absolutely a business requirement to do so.
- Never insert floppy disks, CD's or USB devices that have been in contact with a non **TfGM** PC. If it is absolutely necessary for presentations etc from a third party ensure that they are scanned for viruses by Serviceline before using them.
- Do not attach personal devices to PC's, not even to charge them, as worms and other malware can be spread in this way.
- New viruses are discovered almost every day. If you suspect your PC may be infected with an undetected virus please report to Serviceline

7 Definitions

Anti-Virus Software: An application used to protect computer from viruses, typically through real time defences and periodic scanning. Antivirus software has evolved to cover other threats, including Trojans, spyware, and other malware.

Macro: a macro is a rule or pattern that specifies how a certain input sequence should be mapped to an output sequence according to the defined procedure.

Malware: short for malicious software, is a software designed to secretly access a computer system without the owners informed consent. Intrusive, or annoying software or program code.

Spam Mail: Also known as junk mail, or unsolicited bulk e-mail is a subset of spam that involves nearly identical messages sent to numerous recipients by email.

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

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