Transport for Greater Manchester

Transport for Greater Manchester Policy

IS E-mail 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 E-mail Policy Ref No. 10
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

Table of Contents

1 Policy Aims

a) The purpose of this policy is to detail TfGM acceptable usage of the email service and describe the standards that are required when using email.

b) This policy will help TfGM reduce risk of an email-related security incident, foster good business communications both internal and external to TfGM and provide for consistent and professional application of TfGM email principles.

2 Policy Scope

a) Email is an essential component of business communication; however it presents a particular set of challenges due to its potential to introduce a security threat to the network.
b) Email can also have an effect on the TfGM's liability by providing a written record of communications. This policy outlines expectations for appropriate, safe, and effective email use.

c) The scope of this policy includes TfGM's email system in its entirety, including desktop and/or web-based email applications, server-side applications, email relays, and associated hardware. It covers all electronic mail sent from the system, as well as any external email accounts accessed from the company network.

The policy applies to all permanent and temporary employees, contractors, consultants and 3rd Parties who have access to TfGM's email system.

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

Information including dates, times, duration and device identity will be logged and maybe used for monitoring purposes, should a breach of policy be identified, it may be used in disciplinary proceedings.

6 Policy

6.1 Proper Use of the E-mail System

Users must adhere to the IS Confidential Data Policy, exercise common sense when sending or receiving email and adhere to the following principles to ensure the proper use of the email system. Under no circumstances should credit/debit card data be sent using the TfGM email system, e.g. the 16 digit number with or without the expiry date or CVV.

6.2 Sending Email

When using a TfGM email account, email must be addressed and sent carefully. Users should keep in mind that TfGM loses any control of email once it is sent external to the network. Users must take extreme care when typing in addresses, particularly when the email address auto-complete features are enabled; using the "reply all" function; or using distribution lists in order to avoid inadvertent information disclosure to an unintended recipient. Careful use of email will avoid the unintentional disclosure of sensitive or non-public information.

6.3 Personal Use and General Guidelines

Personal usage of the TfGM email system is permitted as long as such usage does not negatively impact:

- the computer network
- the user's job performance

Any personal emails sent or received via the TfGM email system will not be released by Serviceline should they be blocked by Content Control.

The following types of emails are never permitted to be sent or forwarded on the TfGM email system:

- spamming
- harassment
- communicating threats
- solicitations
- chain letters
- pyramid schemes

Note: This list is not exhaustive, but is included to provide a frame of reference for types of activities that are prohibited.

The user is prohibited from forging email header information or attempting to impersonate another person.

Email is an insecure method of communication, and thus information that is considered confidential or proprietary to TfGM may not be sent via email, regardless of the recipient, without proper encryption.

It is TfGM policy not to open email attachments from unknown senders, or when such attachments are unexpected.

Email systems were not designed to transfer large files and as such emails should not contain attachments of excessive file size.

Note: that the topics above may be covered in more detail in other sections of this policy.

7 Business Communications and Email

TfGM uses email as an important communication medium for business operations. Users of the corporate email system are expected to check and respond to email in a consistent and timely manner during business hours.

Additionally, users are asked to recognise that email sent from a TfGM account reflects on TfGM, and, as such, email must be used with professionalism and courtesy.

8 E-mail Signature

An email signature (contact information appended to the bottom of each outgoing email) is required for all emails sent from TfGM email system and must take the format found on the Intranet via Library – Corporate Templates – Email Signature.

9 Out of Office Auto-Responders

TfGM requires the use of an auto-responder if the user will be **out of the office** for an entire business day or more. The auto-response should notify the sender that the user is out of the office, the date of the user's return, and who the sender should contact if immediate assistance is required, for example:

> "I will be out of the office until [Date of Return]. If your request is urgent and you require assistance during my absence please email [Alternative contacts email address and/or phone number].

The out of office message must be professional and not include any unnecessary text.

10 Mass Emailing

TfGM makes the distinction between the sending of mass emails and the sending of unsolicited email (spam). Mass emails may be useful for both sales and non-sales purposes (such as when communicating with TfGM's employees or customer base), and is allowed as the situation dictates. The sending of spam is strictly prohibited.

It is TfGM's intention to comply with applicable laws governing the sending of mass emails. For this reason, as well as in order to be consistent with good business practices, TfGM requires that marketing or newsletter type emails sent to recipients external to TfGM have the following characteristics:

- The email must contain instructions on how to unsubscribe from receiving future emails (a simple "reply to this message with UNSUBSCRIBE in the subject line" will suffice). Unsubscribe requests must be honoured immediately.
- The email must contain a subject line relevant to the content.
- The email must contain contact information, including the full physical address, of the sender.
- The email must contain no intentionally misleading information (including the email header), blind redirects, or deceptive links.

11 Opening Attachments

Users must use care when opening email attachments. Viruses, Trojans, and other malware can be easily delivered as an email attachment. Users must:

- Never open unexpected email attachments.

- Never open email attachments from unknown sources.
- Never click links within email messages unless he or she is certain of the link's safety. It is often best to copy and paste the link into your web browser, or retype the URL, as specially-formatted emails can hide a malicious URL.

TfGM will use methods to block what it considers to be dangerous emails or strip potentially harmful email attachments as it deems necessary.

12 Monitoring and Privacy

Misuse of email can have a detrimental effect on other users and, potentially, on TfGM public profile. Users should not expect privacy when using TfGM 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 computer network. To ensure compliance with company policies TfGM may with reasonable justification, intercept, monitor and/or review any email, or other messages sent or received, this also includes the data stored on personal file directories, hard disks, and removable media.

13 Company Ownership of Email

Users should be advised that TfGM owns and maintains all legal rights to its email systems and network, and thus any email passing through these systems is owned by TfGM and it may be subject to use for purposes not anticipated by the user. Keep in mind that email may be backed up, otherwise copied, retained, or used for legal, disciplinary, or other reasons. Additionally, the user should be advised that email sent to or from certain public or governmental entities may be considered public record.

14 Contents of Received Email

Users must understand that TfGM has little control over the contents of inbound email, and that this email may contain material that the user finds offensive. Provisions are in place to reduce the amount of unsolicited email that the users receive, however no solution will be 100% effective. It is important that the user does not open emails, reply or click links within the email that, in the user's opinion, seem suspicious. If the user is particularly concerned about an email, or believes that it contains illegal content, he or she should notify the IS Service Desk.

15 Access to Email from Mobile Phones

Many mobile phones or other devices, often called smartphones, provide the capability to send and receive email. This can present a number of security issues, particularly relating to the storage of email, which may contain sensitive data, on the phone. Users are not to access, or attempt to access, TfGM email system from a mobile phone without completing a Mobile Access Request Form. This does not include access to email using the Outlook Web Access platform.

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.

16 Email Regulations

Specific regulations relating to the company's use or retention of email communications are listed below:

- Data Protection Act 2018
- Freedom of Information Act 2000
- PCI-DSS Regulations

17 External and/or Personal E-mail Accounts

TfGM recognises that users may have personal email accounts in addition to their TfGM provided account. The following sections apply to non-TfGM provided email accounts:

17.1 Use for Company Business

Users must use the TfGM email system for all business-related email. Users are prohibited from sending business email from a non-TfGM-provided email account. This includes the transmission of emails to and from personal accounts for all documents that are not classified as ‘public’.

17.2 Use for Personal Reasons

Users are strongly encouraged to use a non-TfGM-provided email account for any non-business communications. Business communications must not be sent either individually or using an auto-forward rule to a non-TfGM provided email address.

18 Confidential Data and Email

The following sections relate to confidential data and email:

18.1 Passwords

As with all TfGM passwords, passwords used to access email accounts must be kept confidential and used in adherence with the IS Password Policy. At the discretion of the IS Department, TfGM may further secure email with certificates, two factor authentication, or other security mechanisms.

18.2 Email Confidential Data

Email is an insecure means of communication. Users should think of email as they would a postcard, which, like email, can be intercepted and read on the way to its intended recipient.

TfGM requires that any email containing confidential information sent external to TfGM be encrypted using commercial-grade, strong encryption. Encryption is encouraged, but not required, for emails containing confidential information sent internal to TfGM. When in doubt, encryption should be used. For information on how to use email encryption, contact Serviceline.

Further guidance on the treatment of confidential information exists in the company's IS Confidential Data Policy. If information contained in the Confidential Data Policy conflicts with this policy, the Confidential Data Policy will apply.

19 Company Administration of E-mail

The IS Department will administer TfGM’s email system in a manner that allows the user to both be productive while working as well as reduce the risk of an email-related

security incident.

19.1 Filtering of Email

A good way to mitigate risk from email is to filter it before it reaches the user so that the user receives only safe, business-related messages. For this reason, TfGM will filter email at the Internet gateway and/or the mail server, in an attempt to filter out spam, viruses, or other messages that may be deemed

- contrary to this policy, or
- a potential risk to TfGM IS security.

No method of email filtering is 100% effective, so the user is asked additionally to be cognisant of this policy and use common sense when opening emails.

Additionally, emails identified as suspicious will be quarantined and/or automatically deleted.

19.2 Email Disclaimers

The use of an email disclaimer, text appended to the end of every outgoing email message, is an important component in the TfGM risk reduction efforts. TfGM requires the use of email disclaimers on every outgoing email as defined below:

> *NOTE: This email message and any attachments are for the sole use of the intended recipient(s) and may contain confidential and/or privileged information. Any unauthorised review, use, disclosure or distribution is prohibited. If you are not the intended recipient, please contact the sender by replying to this email, and destroy all copies of the original message.*

TfGM must periodically review any applicable regulations relating to its electronic communication to ensure that its email disclaimer includes all the required information.

19.3 Email Deletion

Users are encouraged to delete email periodically when the email is no longer needed for business purposes. This ensures that the size of the user's email

account remains manageable, and reduces the burden on TfGM to store and backup unnecessary email messages.

Users must ensure that they frequently empty the email 'deleted items' folder to permanently remove the email from the mailbox.

TfGM enables the 'recover deleted items' tool to be used to recover items deleted from the mailbox for a period of 10 days.

Users are strictly forbidden from deleting email in an attempt to hide a violation of this or another TfGM policy. Further, email must not be deleted when there is an active investigation or litigation where that email may be relevant.

19.4 Retention and Back-up

Email should be retained and backed up in accordance with the applicable policies, which may include but are not limited to the: IS Data Classification Policy, IS Confidential Data Policy, IS Backup Policy, and IS Retention Policy.

Unless otherwise indicated, for the purposes of backup and retention, email should be considered operational data.

19.5 Address Format

To simplify email communication as well as provide a professional appearance email addresses must be constructed in a standard format in order to maintain consistency across the company as defined below:

Firstname.lastname@TfGM.com

Where there is a duplication of an email due to two employees with the same name then an appropriate variation to the email address format is allowed.

19.6 Email Aliases

The use of an email alias, which is a generic address that forwards email to a user account, must be used when the email address needs to be in the public domain,

such as on the Internet. Aliases reduce the exposure of unnecessary information, such as the address format for TfGM email, as well as the names of TfGM employees who handle certain functions. Keeping this information private can decrease risk by reducing the chances of a social engineering attack.

19.7 Account Activation

Email accounts will be set up for each user determined to have a business need to send and receive email. Accounts will be set up at the time a new hire starts with TfGM, or when a promotion or change in work responsibilities for an existing employee creates the need to send and receive email.

At times, email accounts may be given to non-employees, contractors, or other individuals authorised to conduct certain aspects of TfGM business. In these cases, TfGM must designate the temporary or non-employee status of the account in the account display name.

19.8 Account Termination

It is the Managers responsibility to inform the IS Service Desk when a member of staff leaves TfGM, or their email access is officially terminated for another reason, The IS Department will disable the user's access to the account by password change, disabling the account, or another method. TfGM is under no obligation to block the account from receiving email, and may continue to forward inbound email sent to that account to another user, or set up an auto-response to notify the sender that the user is no longer employed by TfGM.

19.9 Storage Limits

As part of the email service, email storage may be provided on TfGM servers or other devices. The email account storage size must be limited to what is reasonable for each employee, at the determination of the IS Department up to a maximum of 2 GB. Storage limits may vary by employee or position within TfGM.

20 Prohibited Actions

The following actions shall constitute unacceptable use of the email system. This list is not exhaustive, but is included to provide a frame of reference for types of activities that

are deemed unacceptable. The user may not use the corporate email system to:

1 Send any information that is illegal under applicable laws.
2 Access another user's email account without:
- the knowledge or permission of that user - which should only occur in extreme circumstances, or
- the approval of company executives in the case of an investigation, or
- when such access constitutes a function of the employee's normal job responsibilities.
- the approval of the users line manager in the event that the user is unobtainable and there is a requirement to immediately retrieve emails that would otherwise negatively impact on TFGM.
3 Send any emails that may cause embarrassment, damage to reputation, or other harm to TfGM.
4 Disseminate defamatory, discriminatory, vilifying, sexist, racist, abusive, rude, harassing, annoying, insulting, threatening, obscene or otherwise inappropriate messages or media.
5 Send emails that cause disruption to the workplace environment or create a hostile workplace. This includes sending emails that are intentionally inflammatory, or that include information not conducive to a professional working atmosphere.
6 Make fraudulent offers for products or services.
7 Attempt to impersonate another person or forge an email header.
8 Send spam, solicitations, chain letters, or pyramid schemes.
9 Knowingly misrepresent the company's capabilities, business practices, warranties, pricing, or policies.
10 Conduct non-TfGM-related business.
11 Images or text which would breach a third party intellectual property rights
12 Material that could be considered libellous, harassing, threatening or defamatory.
13 commercial material unrelated to TfGM and its line of business.
14 bulk non-commercial e-mail unrelated to TfGM or its business.
15 unsolicited e-mail messages (spam).
16 E-mail messages purporting to originate from someone other than the original sender (spoofed messages).
17 Material of a discriminatory nature (including but not limited to sexist, homophobic, racist, pornographic or otherwise offensive content).
18 Any material that indirectly or directly condones criminal activity.
19 Messages or attachments that could damage TfGM's reputation.
20 Material that is likely to prejudice or seriously impede the course of justice in UK criminal or civil proceedings.
21 Material that contains personal information (Defined by the Data

Protection Act 2018) about third parties unless their permission has been explicitly given.

22 Send Primary Account Number (PAN) data under PCI-DSS (i.e. the 16 digit credit/debit card number and with or without expiry date or CVV.

TfGM may take steps to report and prosecute violations of this policy, in accordance with TfGM standards and applicable laws.

20.1 Data Leakage

Data can leave the network in a number of ways, often this occurs unintentionally by a user with good intentions. For this reason, email poses a particular challenge for TfGM to maintain control of its data.

Unauthorised emailing of TfGM data, confidential or otherwise, to external email accounts for the purpose of saving this data external to TfGM systems is prohibited. If a user needs access to information from external systems (such as from home or while travelling), that user must use a mobile working solution provided by the IS Department and must not email the data to a personal account or otherwise remove it from any TfGM systems.

TfGM may employ data loss prevention techniques to protect against leakage of confidential data at the discretion of the IS Department.

20.2 Sending Large Emails

Email systems were not designed to transfer large files and as such emails should not contain attachments that exceed 10Mb. The email system will limit the sending of emails that are in excess of the 10Mb limit.

Sending emails with attachments to large distribution groups has an additive effect and increases the overall storage requirements for the email system. If attachments need to be shared with internal recipients then the files should be stored in a shared folder, the email should then contain a link to the file. This is especially important when there are multiple internal recipients. When sending to external recipient's restraint must be used for sending large files to more than one person.

21 Enforcement

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

22 Definitions

Auto Responder: An email function that sends a predetermined response to anyone who sends an email to a certain address. Often used by employees who will not have access to email for an extended period of time, to notify senders of their absence.

Certificate: Also called a "Digital Certificate." A file that confirms the identity of an entity, such as a company or person. Often used in VPN and encryption management to establish trust of the remote entity.

Data Leakage: Also called Data Loss, data leakage refers to data or intellectual property that is pilfered in small amounts or otherwise removed from the network or computer systems. Data leakage is sometimes malicious and sometimes inadvertent by users with good intentions.

Email: Short for electronic mail, email refers to electronic letters and other communication sent between networked computer users, either within a company or between companies.

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

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

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

Spam: Unsolicited bulk email. Spam often includes advertisements, but can include malware, links to infected websites, or other malicious or objectionable content.

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

Two Factor Authentication: A means of authenticating a user that utilises two methods: something the user has, and something the user knows. Examples are smart cards, tokens, pin numbers or biometrics, in combination with a password.

- *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	31/03/2014	C Burke
3.1	Minor revisions and clarifications	PCI-DSS requirements	20/08/2014	D Johnston
3.2	Reference “personal” changed to “non-TfGM provided”	Clarification	17/10/2014	D Johnston
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	Data protection law	Annual Review	31/03/2019	C. Styler