Transport for Greater Manchester

Transport for Greater Manchester Policy

IS Classification 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 Classification Policy Ref No. 006
Version No.	8.0	Prepared by:	Michelle Peel
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 a method for classifying data and to specify how the data must be handled once it has been classified in order that TfGM complies with its obligations with the Data Protection Act (2018).

b) Information assets are assets to TfGM just like physical property. In order to determine the value of the asset and how it should be handled, data must be classified according to its importance to TfGM operations and the confidentiality of its contents. Once this has been determined, TfGM can take steps to ensure that data is treated appropriately.

2 Policy Scope

The scope of this policy covers all TfGM information stored on TfGM-owned, TfGM-leased, and otherwise TfGM-provided systems and media, regardless of location. Also covered by the policy are hardcopies of TfGM data, such as printouts, faxes, notes, etc.

3 Policy Delivery

The 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

All managers are responsible for classifying information within their department.
Should a breach of this policy be identified, it may be used in disciplinary proceedings.

6 Policy - Information Processing

All information users must comply with the eight Data Protection Principles, as referenced by the Data Protection Act 2018, that define how information can be legally processed. 'Processing' includes obtaining, recording, holding or storing information and carrying out any operations on the information, including adaptation, alteration, use, disclosure, transfer, erasure, and destruction.

1. Personal information shall be processed fairly and lawfully.
2. Personal information shall be held only for one or more specified and lawful purposes and shall not be further processed in any manner incompatible with that purpose or purposes.
3. Personal information shall be adequate, relevant and not excessive in relation to the purpose for which it is processed.
4. Personal information shall be accurate and where necessary kept up to date.
5. Personal information processed for any purpose shall not be kept for longer than is necessary for that purpose.
6. Personal information shall be processed in accordance with the rights of information subject under the DPA.
7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal information and against accidental loss or destruction of the information.
8. Personal information shall not be transferred to a country or a territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal information (refer to Data Protect Policy and Code of Conduction for more information).

6.1 Information Classification

Information residing on **TfGM's** systems must be continually evaluated and classified into one of the following categories:

1. **Non-Classified:** includes user's own information, emails, documents, released marketing material, commonly known information or information already in the public domain.

2. **Operational:** any information required for basic business operations, communications with vendors, employees, etc. (non-confidential).

3. **Critical:** any information deemed critical to TfGM operations.

4. **Confidential:** any information deemed proprietary to TfGM, 'Personal' information, sensitive to TfGM, sensitive to an individual, may be misinterpreted if viewed by none authorised individuals or related to racial/ethnic origin, political opinion, religious or similar beliefs, trade union membership, physical or mental health or condition, sexual life and criminal records.

6.2 Information Storage

The following apply to the storage of the different types of information classifications.

1. Non-Classified

All information that is related to TfGM business must be stored on a network location, within an application or database. Information that is owned and related only to a user has no requirements for storage.

2. Operational

All operational information must be stored within the Quality Management System or TfGM IS systems.

3. Critical

All critical information must be stored within the Quality Management System or TfGM IT systems.

4. Confidential

All confidential information must be removed from desks, computer screens, and common areas unless it is currently in use. Confidential information must be strictly controlled and stored in a secure location. Access to confidential information must only be granted to authorised personnel.

6.3 Data Transmission

The following apply to the transmission of the different types of information classifications.

1. Non-Classified

There are no requirements for 'non-classified' information.

2. Operational

Operational information must be marked as uncontrolled when not in the Quality Management System.

3. Critical

Critical information must be marked as uncontrolled when not in the Quality Management System. All electronic methods of transmission outside of TfGM must utilise an IS approved encryption method.

4. Confidential

An Information Transfer form must be signed by the Information Owner, relevant Manager or Director before transferring the Information outside of TfGM.

All electronic methods of transmission outside of TfGM must utilise an IS approved encryption method. For non-electronic information transfers a method that returns a delivery receipt must be used.

6.4 Information Destruction

The following apply to the destruction of the different types of information classifications.

1. Non-Classified

There are no requirements for the destruction of Non-classified information.

2. Operational

There are no requirements for the destruction of Operational Information, though shredding is encouraged.

3 Critical

There are no requirements for the destruction of Critical Information, though shredding is encouraged.

4. Confidential

Confidential information must be destroyed in a manner that makes recovery of the information impossible. The process must be audit trailed.

7 Information Security

All users of confidential information must ensure that all confidential information they hold is kept securely. They must ensure that it is not disclosed to any unauthorised third party in any form either accidentally or otherwise.

8 Enforcement

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

9. Definitions

Authentication: A security method used to verify the identity of a user and authorise access to a system or network.

Backup: To copy data to a second location, solely for the purpose of safe keeping of that information.

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

Mobile Data Device: A information storage device that utilises flash memory to store information, often called a USB drive, flash drive, or thumb drive.

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, 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
4.0	Date & Version	Annual Review	30/04/2015	C Burke
5.0	Date & Version	Annual Review	31/03/2016	C. Burke
6.0	Date & Version	Annual Review, Head of IS Change	31/03/2017	C. Burke
7.0	Date and Version	Annual Review	31/03/2018	C. Styler
8.0	Updates, Date and Version	Annual Review & change of data protection law year	31/03/2018	C. Styler