Transport for Greater Manchester

Transport for Greater Manchester Policy

IS Disposal of Confidential Waste 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 Disposal of Confidential Waste Ref No. 008
Version No.	8.0	Prepared by:	Michelle Peel
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: 31st January 2020

Table of Contents

1 Policy Aims

This policy governs the disposal of any waste material that contains information that would constitute a breach of confidentiality if it became available to unauthorised persons – confidential waste.

2 Policy Scope

TfGM produces and handles a vast amount of information as part of its activities. Some of this information is confidential in its nature and needs to be disposed of in a secure manner to prevent unauthorised disclosure.

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

Line Managers should ensure compliance within their sphere of responsibilities and control.

6 Policy

As a rule of thumb, the following criteria should be observed when deciding whether information should be classified as being confidential:

Would disclosure of the contents:

- Result in the identification of a service user, or member of staff and thereby breach rules of confidentiality and data protection?
- Provide information to a third party, which could result in legal action being taken against the TfGM?
- Provide statistical, research, financial or other information which could compromise the business capabilities of the TfGM?

Examples include:

- Information relating to a particular employee, former employee or applicant to become an employee. Including personnel records, payroll records, job applications, appraisal forms, internal communication, reports, expense claims, references etc.
- Information relating to any existing or formers applicants or recipients of any service provided by TfGM, such as concessionary passes and permits.
- Information supplied by any particular person in response to consultation requests.
- Information relating to any existing or former applicants or recipients of any financial assistance provided by TfGM, e.g. disturbance claims under compulsory purchase legislation.
- Information relating to any particular individual contained in confidential internal communications.
- Information relating to any particular claimant or claim against TfGM under the provisions of its insured or uninsured liabilities.
- Any information arising from internal audit or other investigation.
- Information relating to the financial or business affairs of any particular person or company e.g. claims for loss of business under compulsory purchase legislation, information on the commercial standing of suppliers.
- Information concerning any terms proposed by or to TfGM in the course of negotiations for the acquisition or disposal of property or the supply of goods or services. Any instructions to counsel and any opinion of counsel and any advice or information obtained or action taken in connection with legal disputes or proceedings.
- Details of commercial terms or information relating to any contract or arrangement which is the subject of a Confidentiality Agreement.

- Information contained in reports to the Executive Board or listed under Appendix 3 of the Local Government Act 1972 (Part B – Confidential Reports).
- Information contained in research and planning documents, the subject of which may give rise to blight of property or otherwise contains confidential information relating to strategic planning or financial issues.
- Information relating to bank details and payment details.

This procedure relates to all confidential information regardless of its format, including; paper, computer files, DVD's, CD's, Memory Sticks, CCTV footage, microfilm etc. Irrespective of how the information is held, all staff are responsible for ensuring that, when required, confidential information is disposed of securely.

The following legislation and guidance include references to the requirement for the secure disposal of confidential information:

- Data Protection Act 2018;
- Human Rights Act 1998;
- The Computer Misuse Act 1990;
- Electronic Communications Act 2000;
- Privacy and Electronic Communications Regulations 2003;
- ISO 27001 Information Technology – Code of Practice for Information Security Management.

All staff working for or on behalf of the TfGM are responsible for complying with these guidelines and disposing of their confidential waste appropriately.

7 Procedure

- Before disposing of confidential waste, consult the corporate retention and disposal schedule to help ascertain as to whether the information needs to be retained for a period of time. If it needs to be retained and is in a hard copy format, consider boxing it and storing at our off-site storage facility.

- Confidential waste must be kept secure and protected against accidental loss, damage or unauthorised access up until its final destruction:

- Confidential/sensitive paper information must be disposed of by using the secure green confidential waste bins. The content of these green bins are collected by the Porters on a monthly basis and their contents securely destroyed by our contractor.

- The confidential waste bins should only be used for confidential paper waste and any other sensitive paper material. They should not be used for the disposal of general domestic waste. The cost of destruction of confidential waste is high and based on weight. Non-confidential/sensitive information should be disposed of in the normal way.

- Paper or computer print outs containing confidential information should never be used for "scrap" or disposed of in waste paper bins.

- CD/DVD's, memory sticks or other removable storage media that contain confidential/sensitive information should be encrypted and kept in a locked filing cabinet, drawer, or safe. Confidential/sensitive information should only be kept on this media for a short period of time and when no longer required, removed from the device promptly. Should you require any assistance with removing files from this media, please contact Serviceline on extension 701234.

- All computers should have their contents wiped before being either re-issued or disposed of.

- Any breach of the procedure should be classed as an information security breach incident and reported in accordance to the TfGM's information incident reporting policy.

8 Roles and Responsibilities

All individuals working for or on behalf of TfGM should follow this procedure.

Line Managers should ensure compliance within their sphere of responsibilities and control.

Porters are responsible for collecting the green bins and returning them to departments when emptied.

Our confidential waste contractor is responsible for collecting our confidential waste and disposing of it in a secure manner.

TfGM's Information Manager is responsible for developing, communicating and maintaining this procedure.

9 Further Guidance

Further advice and guidance on this policy or any other aspect of information management is available from TfGM's Information Manager – (ext. 1123 ,michelle.brown@tfgm.com)

Change Control Record

Policy/Procedure:				
Version	**Change**	**Reason for change**	**Date**	**Name**
V0.1	Draft developed and shared with key IS stakeholders, Internal Audit and Howard Hartley for comments.		29/11/10	Craig Berry
V0.2	Confidential/sensitive information being kept on portable media should only be kept for a short time. Serviceline can be contacted to remove files.	Incorporated comments received from Internal Audit.	09/12/10	Craig Berry
V0.3	Change of date and Version	Annual review	31/03/2014	C Burke
V.4	Change of date and version	Annual review	30/04/2015	C Burke
V.5	Change of date and version	Annual review	31/03/2016	C Burke
V.6	Change of date and version	Annual review & new head of IS	31/03/2017	C. Burke
V.7	Change M. Brown's name and change bin colour	Annual review	31/03/2018	C. Styler
V.8	Change of data protection law	Annual review	31/03/2019	C. Styler