Transport for London

TfL Standard – Information Security Classification

Issue date: 1 July 2010
Effective: 1 July 2010

Table of contents

Part 1: TfL Information Security Classification Standard

Purpose

1. This TfL Standard sets out an information security classification scheme covering information and records, in all formats, held by TfL. The objectives are to:
   (a) Improve the reliability of, and confidence in, the security of our stored information.
   (b) Reduce information risk, including the likelihood of security incidents or data breaches.
   (c) Clarify the categories of information which require secure handling.
   (d) Reduce the burden of determining which information requires secure handling.
2. The Standard is designed to:
   (a) Provide clear guidelines to all TfL Personnel on minimum security standards for the information they manage.
   (b) Provide a set of standard requirements for managing information in accordance with its defined security classification.
   (c) Provide a set of classifications which TfL Personnel must use when labelling unpublished information.

Definitions

3. Information: any information, data or records, irrespective of format, generated or used by a business system or process. Examples include electronic communications, emails, video or digital recordings, hard copy (paper) files, images, graphics, maps, plans and technical drawings.
4. Information Classification: assigning a piece of information to a particular category depending on its content.
5. Information Owners: senior managers, who are responsible for managing the acquisition, creation, maintenance and disposal of TfL's Information and Information Systems within their assigned area of control.
6. Information Risk: that part of TfL's overall risk portfolio which relates to the integrity, availability and confidentiality of Information within TfL.
7. Information Security: the ability to protect the integrity, availability, and confidentiality of information held by TfL and to protect information from unauthorised use, disclosure, modification, accidental or intentional damage or destruction.
8. Information Security Breach: an Information Security Incident where it is confirmed that a stated organisational policy or legal requirement regarding Information Security has been contravened.

9. Information Security Incident: a single or a series of unwanted or unexpected Information Security events that have a significant probability of compromising business operations and threatening information security.

10. Information System: information in all media, hardware, software and supporting networks and the processes and human resources that support its acquisition, storage and communication.

11. Records: information captured in either paper or electronic format and held by an organisation (or person), in pursuance of their activities, business transactions or legal obligations.

12. Secure: an adjective used in this document to define the requirement to manage information in such a way as to minimise the risk of a Security Incident occurring through unauthorised disclosure of or access to information.

13. Transport for London (TfL): the statutory corporation and its operating subsidiaries.

14. TfL Personnel: includes all TfL employees as well as all temporary staff, contractors, consultants and any third parties with whom special arrangements (such as confidentiality and non-disclosure agreements) have been made.

Scope

15. This Standard is consistent with TfL's information governance policies (including but not limited to the Information Security Policy; Information and Records Management Policy; and Privacy and Data Protection Policy).

16. The Standard also complies with the requirements of the Payment Card Industry Data Security Standard (PCI DSS) and the Data Protection Act 1998 covering the secure storage and transmission of data.

17. The classification scheme outlined in this Standard does not apply to information received by TfL which is protectively marked in accordance with the Government Protective Marking Scheme (GPMS), although the GPMS was considered in developing TfL's classification scheme. Such information must be managed in accordance with the Security Policy Framework issued by the Cabinet Office. Detailed guidance on data handling in accordance with this Framework will be made available to TfL Personnel who handle such information.

18. The provisions of this Standard will not, as a rule, be applied retrospectively but will come into force from the date on which the Standard is issued.

19. The Standard includes:

    (a) A description of the classes of information which require protective marking for security purposes.

    (b) Notes on the potential impact on TfL of accidental or deliberate compromise of the various classes of information.

    (c) Examples of information covered by each security classification.

(d) Summary guidance on the storage, circulation and disposal of the various classes of information. More detailed requirements for the secure handling of information are included in the Appendix to this Standard.

Roles and responsibilities

20. TfL will implement all necessary measures to protect the security of information in all formats.
21. TfL's Information Owners are responsible for ensuring that TfL Personnel comply with the procedures outlined in the Standard and with relevant information governance policies.
22. Information Governance is responsible, in consultation with the business, for maintaining this Standard and other corporate Policies/Standards relating to information and records management and producing general guidance on best practice in the management and disposal of information and records**.**
23. Information Management (IM) is responsible for ensuring that TfL's Information Systems are capable of meeting the security/handling requirements associated with the security classification of information processed or stored on them.
24. The TfL Information Risk and Security Network and the Information and Records Management Stakeholder Network are responsible for disseminating advice and guidance on best practice in information security and records management.
25. All TfL Personnel are responsible for managing information responsibly and in accordance with TfL's information governance policies, standards and procedures. This includes responsibility for assigning a security classification to information they produce or create and storing and processing it in accordance with Part 2 of this Standard.

Procedures and processes

26. Any new or revised procedure or process developed by TfL which refers to the creation and processing of information should make reference to this Standard and explicitly address the need to classify the associated information in accordance with the security classification scheme detailed in Part 2.

Approval

27. This Standard was approved at the meeting of the TfL Leadership Team on 22 March 2010.
28. This Standard will be subject to periodic review as considered appropriate by General Counsel.
29. Following an organisational restructure, a number of minor amendments to this Standard were made on 22 May 2012.

Part 2: TfL Information Security Classification Scheme

Note: there is no automatic link between a security classification and an exemption under the Freedom of Information Act (FOIA) or the Environmental Information Regulations (EIRs). A security classification of TfL Restricted or above will be taken into consideration when determining whether an exemption should be applied, but other factors will also affect the outcome of that decision.

Classification: **TfL Unclassified**			
Classification description	**Impact on TfL of accidental or deliberate compromise**	**Examples of information covered by security classification**	**Storage and circulation of information**
Information which: ▪ Could be accessed by any employee of TfL. ▪ Is accessible to TfL customers and the general public. ▪ Where not already publicly available, will as a general rule be provided in response to a request under the FOIA or the EIRs	None.	▪ All material on the websites of TfL and its subsidiary companies. ▪ All material listed in TfL's FOI Publication Schemes. ▪ Published material and archival records held in the TfL Corporate Archives which are classified as open to the public. ▪ All material on Source unless specifically classified as *TfL Restricted* or above. ▪ Corporate policies once approved. ▪ All e-mails and similar electronic messaging technologies other than those classified as *TfL Restricted* or above. ▪ All documents in network shared drives or SharePoint other than those classified as *TfL Restricted* or above. ▪ All information in corporate databases unless classified as *TfL Restricted* or above.	Open access storage and circulation permitted, other than for original material in the Archives which may only be viewed on site (copies may be made available on request).

Classification: **TfL Restricted** (Part 1 - information other than personal data)			
Classification description	**Impact on TfL of accidental or deliberate compromise**	**Examples of information covered by security classification**	**Storage and circulation of information**
Restricted for a specified period of time to authorised persons. Security status will as a general rule be downgraded to "*TfL Unclassified*" after a set period of time, ie once no adverse impact would result from disclosure, based on a risk assessment (eg once a policy is approved and published). If known, this should be recorded alongside the classification. Information may be provided to the general public under the FOIA or the EIRs provided it is first de-classified (after a decision has been made not to apply an exemption under the FOIA or EIRs).	**Medium -** Risk of: ▪ causing financial loss or loss of earning potential or facilitating improper gain or advantage for individuals or companies; ▪ disadvantage in commercial or policy negotiations with others; ▪ undermining the proper management and operations of TfL or other public bodies; ▪ prejudicing the investigation or facilitating the commission of crime; ▪ impeding the effective development or operation of TfL policies, or those of other public bodies; ▪ causing disruption of a number of key transport systems for up to 24 hours.	▪ Commercial eg contracts. ▪ Minutes and papers of closed meetings of the TfL Board, its Committees and Panels. ▪ Management of departmental finances and staff. ▪ Risk management and business continuity plans. ▪ Policy development where availability could prejudice the free and frank exchange of ideas or views. ▪ Information provided under an express or implied guarantee of confidentiality. ▪ Investigations into suspected criminal offences (other than systemic fraud or serious crimes). ▪ Discovered material in relation to litigation unless used or referred to in court. ▪ Information relevant to on-going legal cases where unauthorised disclosure could prejudice the conduct of the case. ▪ Any proceedings for any offence committed or alleged to have been committed, the disposal of such proceedings or the sentence of any court in such proceedings.	Secure storage and a clear desk policy; within shared systems must be restricted to those with authorised access and be given protection from unauthorised access/alteration. Should be processed, transmitted and disposed of securely. It is acceptable to transmit information via email and similar electronic messaging technologies, external or internal post.

Classification: **TfL Restricted** (Part 2 - personal data)			
Classification description	**Impact on TfL of accidental or deliberate compromise**	**Examples of information covered by security classification**	**Storage and circulation of information**
Restricted to authorised persons. Includes personal data and sensitive personal data, as defined by the Data Protection Act 1998, regarding employees, customers and the general public; will be provided to the data subject in response to a subject access request. Security status of personal data will not change until the death of the data subject.	**Medium -** Risk of (continued): ▪ causing distress to individuals; ▪ breach of statutory restrictions on the disclosure of information; ▪ breach of proper undertakings to maintain the confidence of information provided by third parties.	▪ Data about a living individual which is essentially of a biographical nature eg: - Personal contact details. - Bank account details. - Personal comments about an individual. - Oyster journey history data. ▪ Employee records, including: - Staff interview or counselling records. - Redundancy records. - Sick pay records. - Maternity pay records. - Income tax and National Insurance returns. - Salary/pension records. ▪ Sensitive personal data, including information about: - Racial or ethnic origins. - Political opinions. - Religious beliefs or other beliefs of a similar nature. - Trade union membership. - Physical or mental health or condition. - Sexual life.	Secure storage and a clear desk policy; within shared systems must be restricted to those with authorised access and be given protection from unauthorised access/alteration. Should be processed, transmitted and disposed of securely. Sensitive personal data or data relating to an individual's finances should not be transmitted via email or similar electronic messaging technologies unless encrypted. It is acceptable to transmit other personal data via a TfL email account, external or internal post. Internal post should be sealed. Personal data should not be stored on a USB stick or other removable media without prior approval of Information Governance.

Classification: **TfL Confidential**			
Classification description	**Impact on TfL of accidental or deliberate compromise**	**Examples of information covered by security classification**	**Storage and circulation of information**
Restricted for extended periods of time to authorised persons only.	**High -** Significant risk of: ▪ Prejudice to individual security or liberty; ▪ Impeding the investigation or facilitating the commission of serious crime; ▪ Shutting down or otherwise substantially disrupting significant national operations including London's transport infrastructure; ▪ Substantially undermining the financial viability of TfL or other major organisations; ▪ Working substantially against national finances or economic and commercial interests; ▪ Seriously impeding the development or operation of major central/local government policies.	▪ Third party intelligence, information or allegations provided under an express guarantee of confidentiality, relating to alleged or actual criminal activity, including fraud. ▪ Details of current or recent criminal investigations of serious offences or systemic fraud. ▪ IT security procedures. ▪ Building security procedures. ▪ Personnel security procedures. ▪ Documents where release would compromise TfL's ability to safely operate transport services. ▪ Transport infrastructure records eg technical plans and specifications. ▪ Operational disaster plans eg evacuation procedures. ▪ Debit or credit cardholder data comprising a Primary Account Number (PAN) and (if stored in conjunction with the PAN), the cardholder name, service code or expiration date.	Secure storage (locked filing cabinets or safes and rooms) for paper records; shared systems must be restricted to those with authorised access and be given protection from unauthorised access/alteration. Must be processed, transmitted and disposed of securely. Must not be stored on a USB stick or other removable media, without an appropriate level of encryption and prior approval of Information Governance. Must not be transmitted via email or any other electronic messaging technologies unless encrypted. Must be transmitted by post in double envelopes (both sealed): externally via registered mail or courier; internally, by hand direct to the intended recipient.

APPENDIX

TfL Requirements for the Secure Handling of Information

Issue date: 21 December 2010

Effective: 1 February 2011

These requirements have been produced by General Counsel to support compliance with TfL's Information Security Classification Standard. They provide clear guidance on the appropriate handling of information based on the security classification allocated to that information.

Table of contents

1. Key to terms used

Electronic messaging technologies: include email, Office Communicator, Blackberry Messenger.

Information Owners: senior managers, who are responsible for managing the acquisition, creation, maintenance and disposal of TfL's information and information systems within their assigned area of control.

Mobile computing devices: laptops, Blackberrys, PDAs and similar devices.

Removable storage media: include microfilm, CDR, DVD, USB, magnetic tapes, disks, removable hard drives.

Shared systems: include shared network drives, SharePoint, all TfL databases.

2. TfL information security classification labels

- TfL UNCLASSIFIED: no security marking necessary
- TfL RESTRICTED: security marking as specified in this document
- TfL CONFIDENTIAL: security marking as specified in this document

These labels are described in greater detail in TfL's Information Security Classification Standard.

3. Descriptors

Descriptors are additional descriptive terms appended to the main classification label in order to clarify why a particular classification has been assigned eg 'TfL RESTRICTED – SENSITIVE PERSONAL DATA'; 'TfL RESTRICTED – POLICY. Downgrade to TfL UNCLASSIFIED once published'. Use of descriptors is optional and may be tailored to the requirements of the individual business area. For further advice on using descriptors contact: informationassurance@tfl.gov.uk

4. Re-assigning information security classifications

- The information security classifications described in this document are indicative of the sensitivity or otherwise of TfL information and may change over time.
- Re-assigning classifications will occur quite commonly where information is only sensitive for a limited time eg once a policy is approved, or a contract is awarded following a procurement exercise.
- Government information which uses the Government Protective Marking Scheme (GPMS) will retain that classification and be treated in accordance with GPMS Information Handling Requirements issued by the Cabinet Office.
- Information from other organisations (except those which use the GPMS) marked 'Confidential' will be labelled 'TfL RESTRICTED' unless otherwise agreed in writing (for example in a contract, information sharing agreement, or Code of Connection).

5. Retrospective application

TfL information security classifications do not have to be applied retrospectively (ie to legacy information) other than to information which is re-activated for current business use.

6. Where to apply labels to information

Application	System administrator to add to metadata
Database	System administrator to add label to the login screen or as a banner within the database
Electronic Document Management System (EDMS)	System administrator to apply labels in metadata
SharePoint	Administrator to apply labels to individual sites or in document library metadata; where this is not appropriate the Administrator must mandate the application of labels by users (ie to individual documents)
File system	Information Owner or user to apply labels as appropriate: ▪ Electronic folder names – use highest level classification applicable to any of its contents ▪ Cover of hard copy files/folders – use highest level classification applicable to any of its contents
Documents created electronically	▪ User to add in footer (on every page) and on title page/cover if applicable ▪ 'TfL RESTRICTED' and 'TfL CONFIDENTIAL' options to be added to footer of document templates – user to apply relevant classification and delete as appropriate
Documents created manually	Stamped/noted on every page
Email messages	User to add label at the end of the subject line
Other electronic messaging technologies	User to add classification at beginning of body of text
Removable storage media	User to label the storage device itself plus container, using a permanent marker
Verbal information	Instigator to mention at beginning of, or at the appropriate point in, the conversation

7.1 Handling requirements: TfL UNCLASSIFIED - hard copy information	
Security marking	▪ No security marking necessary
Access	▪ Unrestricted access
Storage	▪ Any eg open shelving, desk top
Transmission/ information sharing	▪ Any storage and circulation permitted ▪ Exception: original unpublished material held in the TfL Corporate Archives which may only be viewed on site by prior arrangement (copies may be made available on request)
Disposal	▪ Any method permitted

7.2 Handling requirements: TfL UNCLASSIFIED - electronic information	
Security marking	▪ No security marking necessary
Access	▪ Unrestricted access
Storage	▪ Any information storage system which has been approved by IM for use within TfL
Transmission/ information sharing	▪ Any storage and circulation permitted
Disposal	▪ Any method permitted

8.1 Handling requirements: TfL RESTRICTED - hard copy information	
Security marking	▪ Add security label to cover of file (a stamp marked 'TfL RESTRICTED' is recommended) ▪ If a file/folder contains any information which is 'TfL RESTRICTED' the entire file/folder will need to be marked 'TfL RESTRICTED' ▪ Add security label to individual documents (stamp/note on every page) unless the document is a hard copy of an electronically generated internal document and already has the marking in the footer ▪ Photographs: stamp on back of photograph
Access	▪ Filing systems to have a designated Information Owner responsible for authorising and monitoring access ▪ Restricted to authorised persons ▪ Access should be reviewed by Information Owners on a regular basis ▪ Where access is granted to a third party outside the business, the Information Owner must ensure that a non-disclosure/confidentiality agreement is in place ▪ If accessed in a public place, ensure the information cannot be viewed by others
Storage	▪ To be stored in shelving/cabinets/drawers which are locked when not in use ▪ Not to be left on desks when unattended for long periods or overnight (clear desk policy)
Transmission/ information sharing	▪ Must not be removed from TfL premises unless authorised by the Information Owner(s) ▪ May be transmitted via external or internal post or fax ▪ Photocopies or originals may be shared with authorised persons ▪ If shared by telephone identity of recipient should be established to ensure they are authorised to access the information ▪ May be scanned into a secure storage system (ie which has been approved by IM as having the requisite level of security to handle 'TfL RESTRICTED' information) by users authorised to access that system ▪ Faxes should only be used to transmit personal information where the security status of the receiving machine is assured and the recipient is on standby to receive the fax ▪ Sensitive personal information or information relating to an individual's finances should not be transmitted via fax unless an encrypted fax service is available
Disposal	▪ Non-current 'TfL RESTRICTED' information which needs to be kept for a specified period prior to destruction (eg in accordance with TfL's Information and Records Disposal Schedule) should be either held in a secure on-site area or transferred to a TfL approved external records store where it will be protected through controlled access to the area and a secure physical environment ▪ Must be shredded or placed in security shredding bin ▪ Information to be erased from whiteboards and removed from flip charts and shredded

8.2 Handling requirements: TfL RESTRICTED - electronic information	
Security marking	▪ Documents: add security label 'TfL RESTRICTED' in footer (uppercase Arial, 12 point font) ▪ Excel spreadsheets: add security label 'TfL RESTRICTED' below title ▪ Emails: add security label 'TfL RESTRICTED' at end of the subject line and separated by a hyphen ▪ Other electronic messaging technologies: add security label 'TfL RESTRICTED' at the beginning of the body of the text ▪ Shared systems and databases: where it is not possible to label individual records within a database or system then the whole database or system should be assigned the classification level eg by adding the label to the login screen or having it as a banner within the database/system ▪ DVD/CDR/magnetic tapes - user to label the storage device and container 'TfL RESTRICTED'
Access	▪ Each application or system to have a designated Information Owner responsible for authorising and monitoring access ▪ Shared systems: restricted to those authorised to view 'TfL RESTRICTED' information and protected from unauthorised access/alteration ▪ User access permissions for relevant systems must be clearly documented and regularly reviewed/updated ▪ Where access is granted to a third party outside the business, the Information Owner must ensure that a non-disclosure/confidentiality agreement is in place ▪ Mobile computing devices must be password or pin protected ▪ PCs and mobile computing devices must be locked, logged off the network or shut down when unattended ▪ If accessed in a public place via a mobile computing device, ensure the information cannot be viewed by others
Storage	▪ Any secure information storage system (ie which has been approved by IM as having the requisite level of security to handle 'TfL RESTRICTED' information) ▪ Personal information should not be stored on any removable storage media without prior approval of Information Governance ▪ Sensitive personal data must not be stored on removable storage media or mobile computing devices unless encrypted ▪ Data accessed remotely must not be transferred to external hard drives or removable storage media ▪ All removable storage media should be stored in a locked secure cabinet when not in use
Transmission/ information sharing	▪ If shared by telephone identity of recipient should be established to ensure they are authorised to access the data ▪ Do not send unencrypted email containing personal information unless absolutely unavoidable and then only within the tfl.gov.uk network ▪ May be shared with authorised external users via encrypted email or using an IM approved secure network connection eg VPN or SSL ▪ Email attachments containing personal information should, as a minimum, be winzipped for extra security ▪ If printed, must be collected immediately, unless using a secure device which is swipe card or PIN activated
Disposal	▪ Individuals responsible for disposal must ensure that all media formats are disposed of appropriately and that no duplicate information remains ▪ Removable storage media containing 'TfL RESTRICTED' information must be passed to IM for secure disposal ▪ 'TfL RESTRICTED' information in corporate systems must be disposed of securely by IM in such a way as to ensure that it cannot be reconstituted

9.1 Handling requirements: TfL CONFIDENTIAL - hard copy information	
Security marking	▪ Add security label to cover of file (a stamp marked 'TfL CONFIDENTIAL' is recommended) ▪ If a file/folder contains any information which is 'TfL CONFIDENTIAL' the entire file/folder will need to be marked 'TfL CONFIDENTIAL' ▪ Add security label to individual documents (stamp/note on every page) unless the document is a hard copy of an electronically generated internal document and already has the marking in the footer
Access	▪ Filing systems to have a designated Information Owner responsible for authorising and monitoring access ▪ Restricted to authorised users as determined by the Information Owner ▪ A list of persons authorised to access and/or maintain 'TfL CONFIDENTIAL' information should be kept and reviewed regularly by Information Owners ▪ Appropriate security screening (to be defined by the relevant business area in consultation with HR) is required for individuals who are employed in posts which require regular access to 'TfL CONFIDENTIAL' information ▪ Where access is granted to a third party outside the business, the Information Owner must ensure that a non-disclosure/confidentiality agreement is in place ▪ Must not be accessed in a public place (eg a train, cafe)
Storage	▪ Locked filing cabinets or safes within locked and password controlled rooms ▪ Storage areas containing 'TfL CONFIDENTIAL' information should be locked at all times when not in use ▪ Clear desk policy mandatory whenever workstation unattended
Transmission/ information sharing	▪ Must not be removed from TfL premises by users unless authorised by the Information Owner ▪ Must be transmitted externally via registered mail or courier in double envelopes (both sealed) ▪ Must be transmitted internally by hand direct to the intended recipient double enveloped with security marking on inner envelope ▪ May be scanned into a secure storage system (ie which has been approved by IM as having the requisite level of security to handle 'TfL CONFIDENTIAL' information) by users authorised to access that system ▪ Faxes should not be used unless an encrypted fax service is available and the recipient is on standby to receive the fax ▪ Should not be photocopied unless the user's account is password protected
Disposal	▪ Non-current 'TfL CONFIDENTIAL' information which needs to be kept for a specified period prior to destruction (eg in accordance with TfL's Information and Records Disposal Schedule) must be either held in a secure on-site area or sealed with security tags and transferred to a TfL approved external records store where it will be protected through controlled access to the area and a secure physical environment ▪ Must be shredded or placed in security shredding bin ▪ Information must be erased from whiteboards and removed from flip charts and shredded

9.2 Handling requirements: TfL CONFIDENTIAL - electronic information	
Security marking	▪ Documents: add security label 'TfL CONFIDENTIAL' in footer (uppercase Arial, 12 point font) ▪ Excel spreadsheets: add security label 'TfL CONFIDENTIAL' below title ▪ Emails: all emails in this category will be encrypted but should also include the security marking 'TfL CONFIDENTIAL' at the end of the subject line and separated by a hyphen as an extra security measure ▪ Other electronic messaging technologies: will be encrypted but should also include the security marking 'TfL CONFIDENTIAL' at the beginning of the body of the text ▪ Shared systems: all information in a shared system designated as 'TfL CONFIDENTIAL' will inherit that classification ▪ DVD/CDR/magnetic tapes - user to label the storage device and container 'TfL CONFIDENTIAL'
Access	▪ Each application or system to have a designated Information Owner responsible for authorising and monitoring access ▪ Shared systems: restricted to those authorised to view 'TfL CONFIDENTIAL' information ▪ User access permissions for relevant systems must be clearly documented and regularly reviewed/updated ▪ A list of persons authorised to access and/or maintain information designated 'TfL CONFIDENTIAL' must be kept and reviewed regularly by Information Owners (for their assigned area of control) ▪ Appropriate security screening (to be defined by the relevant business area in consultation with HR) is required for individuals who are employed in posts which require regular access to 'TfL CONFIDENTIAL' information ▪ Mobile computing devices must be password or PIN protected ▪ PCs and mobile computing devices must be locked, logged off the network or shut down when unattended ▪ Where access is granted to a third party outside the business, the Information Owner must ensure that a non-disclosure/confidentiality agreement is in place ▪ Must not be accessed via a mobile computing device in a public place (eg a train, internet cafe)
Storage	▪ A secure storage system (ie which has been approved by IM as having the requisite level of security to handle 'TfL CONFIDENTIAL' information) ▪ Must not be stored on removable storage media unless encrypted and with prior approval of Information Governance ▪ Data accessed remotely must not be transferred to external hard drives or removable storage media ▪ All removable storage media must be stored in a locked secure cabinets (or safe) within a locked room
Transmission/ information sharing	▪ Where information is held outside the source system it must be encrypted ▪ May only be transmitted via telephone in cases of operational emergency ▪ Must not be transmitted via email or similar electronic messaging technologies unless encrypted ▪ If printed, must be collected immediately, unless using a secure device which is swipe card or PIN activated ▪ May only be shared with external agencies/across open public networks via a secure encrypted network connection
Disposal	▪ Information Owners are responsible for ensuring that all media formats/duplicate copies are disposed of appropriately ▪ Removable storage media containing 'TfL CONFIDENTIAL' information must be passed to IM by the Information Owner for secure disposal by triple overwriting or disintegration ▪ 'TfL CONFIDENTIAL' information in corporate systems, backup tapes and hard drives must be disposed of securely by IM so as to ensure that it cannot be reconstituted