



## Information Access Policy

Issue date: 1 April 2010

Effective: 1 April 2010

This supersedes any previous policy.

### Purpose

1. The objective of this policy is to establish a framework that ensures Transport for London (TfL) has in place structures and processes to manage requests to access information held by TfL so as to:
  - (a) Ensure requests are dealt with in compliance with the requirements of the Freedom of Information Act 2000 (FOIA), Environmental Information Regulations 2004 (EIR), Data Protection Act 1998 (DPA) and other information access legislation; and
  - (b) Ensure that TfL employees are aware of their obligations in relation to providing access to information held by TfL in accordance with the law.

### Definitions

2. Data Protection Act (DPA): the Data Protection Act 1998, together with all secondary legislation made under it.
3. Data Subject: an individual who is the subject of Personal Data.
4. Environmental Information Regulations (EIR): the Environmental Information Regulations 2004, legislation that provides a right of access to information about the environment.
5. Freedom of Information Act (FOIA): the Freedom of Information Act 2000, legislation that provides a right of access to general information held by public authorities, together with all secondary legislation made under it.
6. Information: any information, data or records, irrespective of format or medium, which are generated or used by a business system or process. Examples include electronic communications, emails, video recordings, hard copy (paper) files, images, graphics, maps, plans, technical drawings, programs, software and all other types of data.
7. Information Access Request: a request (including a Subject Access Request) from any person for information that falls under the FOIA, EIR or DPA.
8. Information Commissioner: the regulator appointed by the Crown to promote public access to official information and protect personal information.
9. Information Governance: a business unit within General Counsel.

10. 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.
11. Information Risk: that part of TfL's overall risk portfolio which relates to the, integrity, availability and confidentiality of Information.
12. Internal Audit: a business unit within General Counsel.
13. Personal Data: Information which relates to a living individual who can be directly identified from either the information itself, or by combining the information with other data available to TfL. Personal Data includes expressions of opinion and indications of intention, as well as factual information.
14. Subject Access Request (SAR): a request from an individual for access to their Personal Data.
15. Transport for London (TfL): the statutory corporation, Transport Trading Limited and its operating subsidiaries.
16. 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.

### **Organisational scope**

17. This policy applies to TfL and to any commercial organisations or service providers (including agencies or consultancy companies) contracted to carry out work for TfL.

### **Policy statement**

18. TfL will increase openness, promote transparency and demonstrate accountability by proactively sharing information with its customers, employees and the general public.
19. The FOIA and EIR allow individuals or organisations the right to request and, subject to certain exemptions, receive information held by a public authority. TfL falls within the definition of a public authority contained in the FOIA.
20. The DPA gives individuals the right to know what information is held about them, and subject to certain exemptions, receive a copy of that information. It also provides a framework to ensure that personal information is handled appropriately (see TfL Privacy and Data Protection Policy).
21. Any TfL Personnel may be guilty of a criminal offence if they alter, deface, block, erase, destroy or conceal any record held by TfL, with the intention of preventing the disclosure of all, or any part, of the Information that the applicant would have been entitled to under the FOIA, EIR or DPA.
22. The discovery or suspicion of any such offence must be reported immediately to Information Governance and may be referred to the police.
23. This policy applies to all recorded information held by TfL in any format, as well as:

- (a) Information held in non-TfL email accounts used by TfL Personnel during the performance of activities covered by their contract of employment (or a relevant contract for services);
  - (b) Information held by another person/body on behalf of TfL (for Information that falls under the FOIA); and
  - (c) environmental Information held by another person/body under the control of TfL who has responsibility in relation to the environment (eg private companies or public private partnerships) (for Information that falls under the EIR).
24. TfL will adhere to the principles laid out in the following codes of practice, policies and guidance in order to support its compliance with the FOIA, EIR and DPA:
- (a) Secretary of State for Constitutional Affairs' Code of Practice on the discharge of public authorities' functions under Part I of the Freedom of Information Act 2000 (issued under section 45 of the FOIA);
  - (b) Lord Chancellor's Code of Practice on the management of records issued under section 46 of the Freedom of Information Act 2000;
  - (c) Code of Practice on the discharge of the obligations of public authorities under the Environmental Information Regulations 2004 (issued under Regulation 16 of the Regulations);
  - (d) Information Commissioner's range of guidance documents;
  - (e) TfL's suite of Information Governance Policies;
  - (f) TfL's Handling Employee Data Policy; and
  - (g) TfL's Policy on the Disclosure of Personal Data to the Police and other Statutory Law Enforcement Agencies.
25. TfL will comply with all other information governance legislation that may be relevant to the proper provision of access to information.

## **Policy content**

26. TfL's policy is to ensure that:
- (a) Information is provided in a timely manner in response to Information Access Requests, unless a statutory exemption applies;
  - (b) Information not required for a specific legal, business, operational or historical purpose will be disposed of promptly and in an efficient manner, in accordance with corporate records disposal schedules;
  - (c) Structures, systems and processes are in place to manage all Information Access Requests in compliance with the appropriate legislation;
  - (d) Information about its activities is held in officially approved and readily accessible repositories (e.g. any emails relating to TfL business, sent by TfL Personnel from non-TfL email accounts, must be copied to a TfL

email address to ensure they can be accessed in the event of a related Information Access Request);

- (e) In response to Information Access Requests that fall under the FOIA and EIR, applicants are informed whether TfL holds the information requested and provided with it, normally within 20 working days, in the format requested; or informed that TfL refuses to confirm or deny the existence of the information and/or refuses to provide it, if an exemption applies or the request is vexatious or identical to one previously received from the same applicant. Any such refusal must be approved by Information Governance;
- (f) FOIA requests may also be refused if the cost of compliance would exceed an appropriate limit of £450 (there is no corresponding cost limit in the EIR). Any such refusal must be approved by Information Governance;
- (g) Complaints about how an Information Access Request has been dealt with are managed in accordance with TfL's published Internal Review Procedure. Any such complaint must be promptly directed to the Head of Information Governance;
- (h) Procedures are in place which allocate responsibility for coordinating FOIA and EIR responses within TfL;
- (i) TfL will maintain and publish information through FOI Publication Schemes, which commit TfL to make certain information readily available, and explain how the public may access it;
- (j) In response to valid Subject Access Requests made under the DPA, TfL will tell an individual whether it, or someone else on its behalf, is processing that individual's Personal Data, and if so, provide a description of: the Personal Data; the purposes for which they are being processed; and those to whom they are or may be disclosed. TfL will also communicate in an intelligible form all the information which forms any such Personal Data;
- (k) TfL will respond to all Subject Access Requests within 40 calendar days of receipt of a valid request;
- (l) In response to Subject Access Requests, TfL will only refuse to provide a copy of the Personal Data processed and information concerning the processing if an exemption applies. Any such refusal must be approved by Information Governance;
- (m) Personal data is not disclosed to third parties except where disclosures are permitted by, or required by, law;
- (n) When considering whether to disclose Information in response to an Information Access Request, the TfL Personnel involved in that process must take into consideration the security classification attached to the information under TfL's Information Security Classification Standard for protectively marking Information. Information classified according to this Standard must be transmitted, stored and disposed of as required by the Classification Standard and its accompanying guidelines; and

- (o) Information Risk is considered and afforded a priority in decisions within TfL in the same way as financial and operational risk. This will be reflected in corporate and local risk registers. Information Risk will be managed by a process of identifying, controlling, minimising and/or eliminating risks that may affect TfL's information or information systems.

### **Responsibility for access to information**

- 27. Each individual employee is responsible for actively supporting this policy. TfL Personnel are responsible for promptly retrieving information where they are requested to do so for the purpose of responding to an Information Access Request.
- 28. Employees must seek advice in the event of uncertainty in relation to this Policy.
- 29. Information Owners are responsible for ensuring that TfL Personnel within their area of control are aware of this policy and are adequately trained in the handling of Information Access Requests.
- 30. Information Owners are responsible for the assessment and reporting of Information Risk linked to the handling of Information Access Requests within each business unit.
- 31. Information Owners will implement appropriate guidelines within their business unit to ensure compliance with corporate procedures on the handling of Information Access Requests.
- 32. TfL Personnel must familiarise themselves with their obligations via the information access training and communication programme co-ordinated and delivered by Information Governance (specifically e-learning courses and guidance available on TfL's intranet).
- 33. Information Governance is responsible for the interpretation of this policy, for monitoring compliance with the policy and for providing advice and guidance on its implementation.
- 34. Information Governance will be responsible for maintaining TfL's FOI Publication Schemes and for maintaining procedures for answering Information Access Requests.
- 35. Information Governance will be responsible for approving any refusal to provide information in response to an Information Access Request and for the implementation of the Internal Review Procedure.
- 36. Information Governance shall be responsible for liaising with the Information Commissioner's Office on any matter relating to TfL's handling or resolution of an Information Access Request.

### **Procedures/Guidelines/Processes**

- 37. All information held by TfL must be managed in accordance with TfL's:
  - (a) Privacy and Data Protection Policy;

- (b) Information Security Policy;
  - (c) Information and Records Management Policy; and
  - (d) Corporate Archives Policy.
38. Requests for the disclosure of Personal Data for the purpose of the prevention or detection of crime, or the apprehension or prosecution of offenders, will be considered in line with the requirements of the DPA and other applicable legislation, and as set out in TfL's Policy on the Disclosure of Personal Data to the Police and other Statutory Law Enforcement Agencies.
39. This policy will be supported by corporate best practice, guidelines and TfL Standards on managing requests for information, available on TfL's intranet.
40. Internal Audit will perform a periodic audit of the information access processes, procedures and practices of TfL and its service providers to monitor compliance with this policy.

### **Approval and amendments**

41. This policy was originally approved at the meeting of the TfL Leadership Team on 22 March 2010.
42. A number of minor amendments to this Policy were approved at the meeting of the TfL Leadership Team held on 2 May 2012.
43. This policy will be subject to periodic review as considered appropriate by General Counsel.

### **Policy owner**

44. TfL's General Counsel is the designated owner of this policy.