Audit and Assurance Committee

Date: **9 March 2015**

Item: **Policy on Disclosure of Personal Data to the Police and Statutory Law Enforcement Agencies**

This paper will be considered in public

1 Summary

1.1 This paper seeks approval for a revised Policy on the Disclosure of Personal Data to the Police and Statutory Law Enforcement Agencies (SLEAs).

2 Recommendation

2.1 **That the Committee approve a revised Policy (Appendix 1) on the Disclosure of Personal Data to the Police and Statutory Law Enforcement Agencies (SLEAs).**

3 Background

3.1 TfL's existing Policy was approved by the Board in 2006 and it applies to around 16,000 requests a year from the police and SLEAs for the disclosure of personal data. Nearly all of these requests relate to data on our customers collected by our ticketing and CCTV systems. Those requests are handled, respectively, by the Enforcement and On-Street Operations (EOS) directorate in Surface Transport and a British Transport Police (BTP) team on behalf of LU Network Security. Requests must be assessed individually and handled in compliance with the requirements of the Data Protection Act 1998 and the Human Rights Act 1998.

3.2 The Policy has provided a successful framework for TfL's provision of information to the police and SLEAs, enabling agreements on information sharing to be reached with the Metropolitan Police Service, BTP and City of London Police. Through the disclosure of personal data in response to their requests, we have made a significant contribution to the detection and apprehension of offenders, contributing to record low levels of crime on London's public transport with fewer than eight crimes now recorded for every million passenger journeys.

3.3 The existing Policy is to disclose personal data in response to valid requests, where we are satisfied that disclosure is necessary and proportionate and in line with TfL's powers. Priority is given to requests relating to crime prevention or detection on our network. In addition, other public bodies (for example, the Security Service or HMRC) have specific statutory powers requiring us to disclose personal data in particular circumstances or for a particular purpose and these provide a gateway for disclosure irrespective of whether their request relates to crime prevention or detection on our network, or in London more widely.

3.4 The Leadership Team approved the revised Policy on 11 February 2015.

4 Revised Policy

4.1 The revisions to the Policy reflect organisational changes, further legal advice, revised guidance from the Information Commissioner and an expansion in the areas receiving requests from the police and SLEAs. The revised Policy does not alter the intention to disclose data where we are permitted to do so and in fact offers the possibility that more requests will result in the disclosure of data, if resources allow. EOS would like to explore the possibility of recovering the costs incurred in responding to police requests, or requesting resources from the police, given capacity is limited. In the meantime, priority will continue to be given to transport related requests.

4.2 Under the revised Policy an annual report on its operation will be submitted to the Audit and Assurance Committee, as is the case now.

4.3 Once the Policy is approved it will form part of the TfL Management System and be published on the TfL website.

List of appendices to this report:

Appendix 1: Revised Policy on the Disclosure of Personal Data to the Police and Statutory Law Enforcement Agencies (SLEAs).

List of Background Papers:

Policy on the Disclosure of Personal Data to the Police and Statutory Law Enforcement Agencies (SLEAs)
Report on Personal Data Disclosure to Police and Other Law Enforcement Agencies (Audit and Assurance Committee 17 December 2014).

Contact Officer: Howard Carter, General Counsel
Number: 020 3054 7832
Email: HowardCarter@tfl.gov.uk

Appendix 1

Policy on the Disclosure of Personal Data to the Police and Statutory Law Enforcement Agencies

Issue date: XX XXXXXX 2015

Effective: XX XXXXXX 2015

This supersedes any previous policy.

Purpose

1. The objective of this policy is to regulate the disclosure of Personal Data held by Transport for London (TfL), to the police and any Statutory Law Enforcement Agency (SLEA), so as to:

   (a) ensure that TfL discloses Personal Data to the police and SLEAs in compliance with the requirements of the Data Protection Act (DPA) 1998, Human Rights Act (HRA) 1998 and other relevant information governance legislation;
   (b) ensure that TfL discloses Personal Data to the police and SLEAs in a manner that will enhance public trust and confidence in TfL and increase its operational effectiveness; and
   (c) ensure that employees and others acting on behalf of TfL are aware of their obligations when dealing with requests from the police and SLEAs for the disclosure of Personal Data.

Organisational scope

2. This policy covers TfL (the statutory corporation, Transport Trading Limited and its operating subsidiaries and its service providers) who may receive requests from the police and other SLEAs for the disclosure of Personal Data held by, or on behalf of, TfL.

Policy statement

3. It is TfL's policy to disclose Personal Data it holds to the police and SLEAs, when it is required to help address any policing, national security or law enforcement issues affecting:

   (a) public passenger transport services to, from or within Greater London, which are operated by or on behalf of TfL;

   (b) any other transport infrastructure outside Greater London operated by or on behalf of TfL.

4. It is also TfL's policy to disclose Personal Data it holds to the police and SLEAs, when it is required to help address a range of specified policing, law enforcement or national security issues affecting Greater London (but not directly affecting

public passenger transport services to, from or within Greater London, which are operated by or on behalf of TfL).

5. TfL will only disclose Personal Data to the police and SLEAs in accordance with its powers; any other relevant legal requirements; and if it is satisfied that such disclosures are both necessary and proportionate in the context of their stated purpose.

6. The DPA and the HRA apply to TfL's use of Personal Data and will play a central role in determining when it is permissible for TfL to disclose it to third parties.

7. When collecting Personal Data, TfL will make individuals aware that it may be disclosed to the police and SLEAs.

Policy content

8. TfL will only disclose Personal Data in accordance with its legal powers.

9. TfL will seek to act in accordance with the 'Data sharing code of practice' issued by the Information Commissioner.

10. Whenever regular disclosures of Personal Data are envisaged, this policy will be implemented through a formal Information Sharing Protocol with the recipient organisation. These will specify the safeguards applicable to the disclosures.

11. In determining the response to a lawful request made by the police or an SLEA, TfL will ensure that the disclosure is proportionate and carried out in a controlled manner. This will be assessed on a case by case basis.

12. In assessing whether the disclosure of Personal Data is proportionate, the following factors should be considered:

    (a) The volume of the data that has been requested;

    (b) The extent to which disclosure affects, or may affect, an individual's privacy;

    (c) The extent to which disclosure is necessary for the prevention of disorder or crime, for the protection of the rights and freedoms of others, or for another valid purpose recognised in the HRA;

    (d) The degree of connection between the individual that is the subject of the data request and the offence that has occurred or is being investigated;

    (e) Whether the external investigation will be prejudiced if the individual is informed that their Personal Data has been requested.

13. Any arrangements under which the police or an SLEA are given direct access to a TfL system containing Personal Data will be documented under an Information Sharing Protocol and supporting Information Sharing Procedure.

Responsibility for compliance

14. TfL Staff and all staff engaged by TfL's service providers, who are involved in data sharing with the police and SLEAs, are responsible for maintaining compliance with this policy.

15. Enforcement and On-Street Operations (Surface Transport) are responsible for the implementation of this policy; and for providing advice and guidance to other

TfL business units which also have responsibility for evaluating requests and authorising disclosures of Personal Data to the police and SLEAs.

16. TfL Staff should seek advice from their supervisor, line manager or EOS in the event of uncertainty in relation to a request for Personal Data from the police or an SLEA. In every such case, TfL Staff should satisfy themselves that there is a sound legal basis for disclosure.

17. If any TfL business unit responsible for evaluating requests and authorising disclosures of Personal Data to the police and SLEAs subcontract or assign these responsibilities to any party other than TfL, they should ensure that any disclosures are carried out in accordance with this policy; that Information Sharing Procedures are updated; and that a Data Processor Agreement is completed (this may form part of a broader contract for services).

18. Information Governance is responsible for liaising with the Information Commissioner's Office on any matter relating to this Policy.

19. Once Personal Data has been disclosed to the police or an SLEA, the recipient organisation will assume full responsibility as Data Controller for the copy of the Personal Data that they have received.

Procedures/Guidelines/Processes

20. This policy will be supported by Information Sharing Protocols, Information Sharing Procedures, Data Processor Agreements and operational guidelines.

21. Each business unit responsible for evaluating requests and authorising disclosures of Personal Data to the police and SLEAs will adopt procedures to address issues including how to validate and evaluate each request and ensure the confidential and secure handling of requests and associated disclosures.

22. All requests for Personal Data submitted by the police should be made in accordance with current Association of Chief Police Officers (ACPO) guidelines; and all disclosures of Personal Data made by TfL will be consistent with relevant guidance issued by the Information Commissioner.

23. Business units responsible for evaluating requests and authorising disclosures of Personal Data to the police and SLEAs should maintain adequate records of the requests they receive and the action taken.

Definitions

24. Data Controller: the organisation (alone, jointly or in common with other organisations) which determines the manner and purposes for which Personal Data is to be processed.

25. Data Processor: processes data on behalf of the Data Controller (other than an employee).

26. Data Processor Agreement: a contract between the Data Controller and the Data Processor that requires the Data Processor to comply with certain security and other obligations in respect of Personal Data it processes on behalf of the Data Controller.

27. DPA: the Data Protection Act 1998, together with all secondary legislation made under it.

28. Data Subject: an individual who is the subject of Personal Data.

29. EOS: Enforcement and On-Street Operations, a TfL business unit within Surface Transport.

30. Greater London: the area comprising the areas of the London boroughs, the City and the Temples, as defined in section 2(1) of the London Government Act 1963.

31. HRA: the Human Rights Act 1998.

32. Information Governance: a TfL business unit within General Counsel.

33. Information Commissioner: the regulator appointed by the Crown to promote public access to official information and protect personal information.

34. Information Sharing Protocol: an agreement between TfL and one or more partner organisation, which defines the overarching purposes for which they have agreed to share Personal Data; the general principles and legal duties which will govern the sharing of such data; and the processes that will support the exchange of such data.

35. 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. This includes data held manually in paper records, as well as all data held electronically (including email, images and audio recordings). Personal Data also includes expressions of opinion and indications of intention, as well as factual information.

36. SLEA: Statutory law enforcement agency, an organisation other than the police, engaged, on a basis established by statute, in the prevention, detection, investigation or prosecution of criminal activities.

37. Transport for London (TfL): the statutory corporation, Transport Trading Limited and its operating subsidiaries.

38. TfL Staff: 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.

Approval and amendments

39. This policy was approved by the TfL Leadership Team on 11 February 2015.

40. This policy was approved by the TfL Audit and Assurance Committee on XXXXX.

41. This policy will be subject to periodic review as considered appropriate by General Counsel.

Policy owner

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