Transport for London

Electronic Communications (Including Email and Internet) and Equipment Usage Policy

Issue date: 18 May 2007
Effective: 21 May 2007
Updated: 1 October 2010
This supersedes any previous policies

Index

Electronic Communications (Including Email and Internet) and Equipment Usage Policy

1. Introduction

Transport for London (TfL) aims to provide electronic communications technology and equipment which will enable employees to perform their roles to the highest standards. This will contribute to the operational success of the business and the achievement of its vision and objectives. Electronic mail (email), TfL Intranet (Source) and the Internet are essential business tools which employees must use effectively and appropriately.

2. Organisational Scope

Employees of TfL, Docklands Light Railway Limited, Rail for London Limited, London Bus Services Limited, London Buses Limited, Victoria Coach Station Limited who are on TfL employment contracts (Paybands 1-5 and Directors) and those staff on predecessor organisation employment contracts where the individual has transferred to the employment of TfL.

3. Policy Statement

TfL's main purpose in providing facilities for email, internet and electronic communications is to support its business activities. This policy sets standards so that employees understand how email, Source, the Internet and all other electronic and communications equipment should be used. It complies with current legislation and alerts employees to the need to be aware that breaches of this policy may lead to disciplinary action being taken against them. Where such breaches are deemed to be gross misconduct, disciplinary action may result in dismissal.

4. Requirements

4.1 All information and communications (ICT) equipment, in whatever form, relating to TfL's business activities and all information handled by TfL relating to other organisations with which it deals is subject to this policy.

4.2 TfL's ICT resources include the following: any computer (including laptops issued for off-site use), mobile and handheld devices (e.g. Blackberries, PDAs, XDAs etc), server or network equipment and any telephone handset, switchboard or voice network provided or supported by TfL. It also includes any data stored, processed or transmitted on such networks and data/programs stored on TfL's computer systems or on magnetic or optical storage media that is owned and/or maintained by TfL.

4.3 This extends to an employee's own, or a third parties, computer equipment, when employees are working on the Company's business away from TfL's premises, or using such equipment on its premises.

4.4 TfL reserves the right to monitor and/or record individual use of ICT facilities for legitimate purposes to protect against misuse and to ensure system and operational efficiency and integrity. It reserves the right to access individual accounts in circumstances where it has a reasonable belief that there has been a breach of this policy.

4.5 Employees should therefore have no expectation of privacy whilst using ICT facilities, including using company equipment for the purposes of communicating via email or in accessing or passing on information obtained through the Internet. Copies of emails may be disclosed to third parties for legal reasons which may include, amongst others, requests made under the Data Protection Act and/or the Freedom of Information Act or in connection with a Court or Tribunal orders for disclosure.

4.6 TfL reserves the right to temporarily or permanently limit, withdraw or restrict the use of, or access to, any ICT facilities if they are used in a way that contravenes this policy.

4.7 Any information created in the course of employment at TfL becomes the property of TfL and may not be used for any other purpose unless approved by the employee's manager. It is the responsibility of employees to ensure that any such work is managed in accordance with TfL's policies and procedures.

4.8 Employees must take all reasonable steps to safeguard the security of ICT systems and the information contained upon them. This includes not allowing unauthorised users access to ICT systems and protecting them from physical damage. They must only access ICT facilities, including email and the Internet via their personal user account and not use or attempt to use another users' account

5. Responsibilities

5.1 All employees:

- must ensure that they do not download, create or transmit material that is abusive or threatening to others or might be regarded as offensive on the basis of personal characteristics such as race, sex, colour, religion, nationality, gender, disability, sexual orientation or age. Where such material is received or stored on personal equipment and brought into the workplace, employees must not show, print, forward or transfer such material on to TfL equipment whilst on TfL premises
- must report it to their manager immediately if any such material is accessed accidentally
- must normally use these facilities for business purposes only

- may use them for limited personal use provided this does not interfere with their work performance and are outside their normal working hours
- must ensure that their usage of TfL's ICT equipment is lawful.
- should contact the IM Helpdesk and their line manager if there is any evidence of misuse

5. 2 All managers and employees with leadership or supervisory roles:

- must take reasonable steps to ensure that the requirements outlined in this policy are adhered to by their employees and that appropriate, fair and consistent action is taken to deal with any failure to conform to them
- should be aware that they can, in some circumstances, be held liable for illegal acts committed by their staff in connection with the use of email or internet or if they fail to maintain adequate supervision

6. Use of Email and Internet

6.1 Email and the Internet are inherently insecure. Confidential, critical or sensitive information should therefore not be sent via email unless there is no reasonable alternative

6.2 Inappropriate or excessive usage could lead to disciplinary action being taken against an employee

6.3 TfL is unable to control the security of personal webmail accounts (such as Hotmail and Yahoo) so these types of account should be avoided for business purposes unless there is no alternative available

6.4 Employees must only use the TfL standard secured connection to the Internet. Unauthorised connections will be considered a serious breach of security. TfL reserves the right to prevent access to certain internet sites

6.5 Employees should not, in normal circumstances share, distribute or amend relevant sections on Source when working with external parties. When seeking to place material on Source, sign off should be obtained from the relevant department head

7. Computer Security

7.1 Employees must:

- keep passwords confidential, not write them down or disclose them to other members of staff, including ICT staff
- ensure that PC/terminals are locked if left unattended. If leaving PC/terminals for a long time or upon leaving the office, employees should ensure that they log off from the system to prevent unauthorised use in their absence. Unless directed otherwise by IM, employees should also close down all electronic equipment at the end of the working day, in line with TfL's initiatives for a sustainable environment

7.2 Employees must not:

- attempt to circumvent any security controls, determine or identify passwords or breach conditional access systems, whether belonging to TfL, its suppliers or third parties
- modify computer equipment provided to employees or input materials onto the system unless authorised to do so
- use or attempt to use ICT facilities or attempt to access data they are not authorised to use or access
- retain TfL information on any non-TfL equipment unless authorised to do so

8. Software

Employees must:

- ensure that software is used legally and in accordance with licensing agreements. Only approved software may be used on TfL computers. If employees are unsure whether software is approved they should refer to their Line Manager or IM
- ensure that all software used on any of TfL's ICT systems is from a reputable and identifiable source, approved in advance by IM Software. Programs, including unlicensed applications and hacking tools (i.e. programs which provide unauthorised access to other systems) must not be downloaded from the Internet on to TfL ICT systems or sent out via emails
- refrain from infringing third party copyright or licensing requirements when using or copying software for which TfL does not own a current user licence. The making of 'extra' copies of software or the introduction of software packages outside TfL is expressly prohibited
- refrain from using TfL ICT storage provision for personal files, including but not limited to, images, videos and sound files

9. Telephone Usage

9.1 Employees should use TfL telephones (including mobile telephones) for the purposes of TfL business although employees may use telephones to make a reasonable number of personal calls. Use of the telephone system for personal calls is subject to TfL's right to monitor the system for legitimate business purposes. By choosing to use the telephone system to make personal calls, you consent to TfL monitoring such calls. TfL reserves the right to claim reimbursement for personal calls made in the event that this privilege is abused. Excessive use of TfL's telephone system for personal use could also have tax implications for employees

9.2 Employees must comply with all relevant legislation in force regarding the use of mobile telephones such as legislation which prohibits the use of mobile telephones whilst operating any vehicle

10. Support and Advice

Support and advice can be obtained through speaking to your manager or contacting HR Services.

11. Ownership and Review

TfL Group Employee Relations and Engagement

Version 1	Effective 21/05/07	
Version 2	Effective 04/02/08	
Version 3	Effective 01/10/10	To take account of the Equality Act 2010

12. Related Documentation

Employees are encouraged to look at this policy in conjunction with:
Code of Conduct
TfL's Employment Policy
Discipline at Work Policy and Procedure
Bullying and Harassment Policy and Procedure
Computer Security and You http://source.tfl/DoingMyJob/Security/3819.aspx
Requirements for the issue and use of Mobile Phones and Pagers
Group IM Information Security Policy