

G1136 A2

GUIDELINES FOR THE USE OF LUL's INFORMATION AND ELECTRONIC COMMUNICATION (INCLUDING EMAIL AND INTERNET) SYSTEMS AND EQUIPMENT**1. Introduction**

London Underground Limited's (LUL) overall policy defining the use of the above is the [Email and Internet Standard](#). As this is an area of rapidly changing technology and practice, however, we also provide up-to-date guidance and advice about the proper and permitted use of these frequently changing and developing facilities. This is so all staff can be clear about what the company expects of them and what the rules are concerning the use of these facilities.

2. Overview: Why is it important to have controls in this area?

LUL makes a considerable investment in its information technology and communications systems to enable its staff to work efficiently. However, this can also be an area of risk through liability, loss or embarrassment in relation to the misuse of these facilities. These Guidelines are to enable staff to understand and comply with the rules surrounding the use of these resources. Breaching these rules can result in disciplinary action which, if deemed as gross misconduct, may result in dismissal.

3. Who is covered by these Guidelines?

Any person working with or on LUL's information and communications (ICT) equipment (LUL staff, agency staff, consultants, etc).

4. What is meant by information and communications (ICT) equipment?

Currently it includes all of LUL's and TfL's ICT equipment and resources, including any computer (including laptops issued for off-site use) and peripherals (printers, scanners etc), camera, mobile and handheld devices (e.g. Blackberries, PDAs, XDA's, etc), server or network equipment and any telephonic device or voice network provided or supported by LUL and TfL. As technology develops new devices, this will expand; therefore, this should not be considered an exhaustive list.

5. What about the data (details and information) on this hardware?

All data stored, processed or transmitted on such networks and data/programs stored on LUL's computer systems or on any storage device or media that is owned and/or maintained by LUL belongs to LUL. It is also essential to understand that this extends to your own, or a third party's computer equipment, when you are working on LUL's business away from LUL's premises, or using such equipment on its premises.



Staff must comply with this policy when using LUL's e-mail service from any location.

6. Does LUL monitor how its ICT equipment is used?

Yes. LUL (or Group Information Management on LUL's behalf), like practically all other companies, at all times reserve the right to monitor and/or record individual use of ICT facilities for legitimate purposes. These purposes will include:

- to protect against or investigate / detect ICT misuse;
- to ensure system and operational efficiency, security and integrity;
- to detect any computer viruses and to check mail boxes of absent staff (only where this is appropriate);
- accessing individual accounts where it has a reasonable belief that LUL's Standard (and therefore this Guideline) has been breached. This could include investigating internet browser history files, downloads, temporary internet files, deleted e-mails, storage systems, and so on. This is, of course, only done where it is felt there are sufficient grounds, and with the prior formal approval of TfL's "Information Access and Compliance Team" and LUL HR / ER, whose job it is to make sure that such a step is justified in the first place.

7. What about issues of privacy?

None of us should have an expectation of privacy whenever we use LUL and TfL ICT facilities and equipment. This includes using LUL equipment for the purposes of communicating via email or accessing or passing on information obtained through the Internet.

8. Can copies of my e-mails be disclosed to third parties?

Yes, but only where there is a legitimate reason which, amongst others, could include requests made under the Data Protection Act and/or Freedom of Information Act or in connection with Court or Tribunal orders for disclosure.

9. Responsibilities

9.1 All Staff

All staff must ensure that they use LUL ICT facilities for business purposes only, subject to the permissions below. It can be gross misconduct to download, create, store, display or transmit material that is defamatory or offensive, or might be capable of constituting any form of discrimination or criminal offence.

This includes any material of a sexually explicit nature, which LUL deems as offensive, material which includes nudity and any kind of illegal material (e.g. how to make an explosive device). Employees who receive any such material



must not forward it on. Any breaches of these requirements may be regarded as gross misconduct and would normally result in dismissal.

If you receive any such material you must immediately delete it and inform your manager, however If you also find the material received offensive you should contact HR Services immediately.

9.2 All managers and employees with leadership or supervisory roles

Managers and supervisors should take all reasonable steps to ensure that the requirements outlined in these guidelines are adhered to by their staff and that appropriate, fair and consistent action is taken to deal with any failure to conform to them.

The company frequently issues bulletins to remind staff of the standard and rules for using its ICT facilities. At a local level managers can reinforce this with their own messages and in team meetings. If Managers require further advice or guidance, then they should contact their Business Partner.

10. Use of email and the internet

As this is a very important area, we have provided detailed guidance. If you are unclear about anything contained here, then please discuss this with your manager before acting.

- E-mail and the Internet are uncontrolled environments and should not be regarded as secure systems. Staff must, therefore, exercise extreme care when sending confidential or sensitive material by e-mail. Email is not suitable for sensitive / confidential communications unless encrypted. When downloading information, staff must take care to avoid the introduction of viruses or the infringement of third party copyright or licensing requirements.
- Software programs must not be downloaded from the Internet on to a desktop computer. Staff must ensure that any electronic media or hardware (mass storage devices eg. CD ROMs, USB flash drives, disks and so on) which are to be used on any of LUL's systems are virus scanned before being used. This includes any hardware supplied via professional or any other bodies.
- Limited and sensible personal use of e-mail and the Internet may be allowed, provided such use is kept to a reasonable level and:
 - does not interfere with a person's performing their duties (whether this be excessive time, or content incompatible with their employment with, or responsibility to, LU);
 - does not produce excessive amounts of hard copy;
 - Is not unacceptable (obscene material, defamatory material, material offensive on the basis of a protected characteristic under the Equality Act, for example, race, gender, etc')