COMMUNICATIONS & INFORMATION SYSTEMS USE POLICY

Introduction

1. This policy is concerned with the security and authorised use of Information Systems (IS), including mobile telephones and personal digital assistants (PDA), provided to assist employees in the performance of their work duties.

2. Communications tools must be operated in line with Service Response Standards, and relevant health & safety principles e.g. Display Screen Usage (Employee Handbook – Section B12).

3. This policy will not breach an individual's right to privacy.

4. Employees with access to the Government Secure Intranet (GSI) or London Public Services Network (LPSN) must additionally read, and comply with, the GSI/LPSN User Agreement included as Appendix 3.

General Principles

5. Individuals are responsible for ensuring their unique user credentials for all work related information systems, including network access, are kept confidential (i.e. not shared with colleagues or written down and left in a non-secure place) and protected from misuse. Individuals are additionally responsible for locking their workstations when they leave them unattended.

6. Individuals will never:

- Use a colleague's user credentials to gain system access;
- Deliberately introduce viruses or other malware into a system;
- Disable antivirus software or inactivity timeouts set on their computer;
- Attempt to bypass or subvert system security controls, or use them for purposes other than those intended.

7. All communications equipment and information systems provided by the organisation remain City of London property at all times and must not be removed from the business premises without the prior approval of a senior manager (unless the equipment has been provided specifically for authorised mobile / home working arrangements).

8. Whilst equipment and systems are provided for organisational use, limited and reasonable personal use will be permitted provided it does not negatively impact on service delivery (see also Internet Access Statement and e-mail Usage Statement). Personal usage is a privilege which could be withdrawn if abused.

9. Software must be used within the scope of the copyright.

10. Employees must minimise the possibility of introducing malicious software to the City of London's information systems e.g. by not opening unreliable or unknown data sources via e-mail or the internet.

11. City of London data must be stored on the IS infrastructure only, in accordance with Data Protection principles. Work carried out on equipment without access to the network must be backed up regularly, uploaded to the network at the earliest opportunity and deleted from local drives. Temporary storage of data on non-City of London equipment is permitted in limited circumstances only – contact the departmental IS team for details.

12. Data must only be copied to removable or mobile media (e.g. laptop, USB, DVD, CD, PDA, mobile phone etc) after an assessment of the risk of the device being lost or stolen has been made (i.e. consideration should be given to the sensitivity of the data). Published IS advice should be followed e.g. IS Advice on Data Security, IS Advice – Risk Analysis for Sensitive Data.

13. Limited (less than 10mb) non-work related data may be stored on the City of London's IS infrastructure at the individual's own risk. Under no circumstances, however, should it be used to store unauthorised software or illegal copies of data such as music, films or images.

14. City of London staff must comply with the principles of Freedom of Information, especially in terms of appropriate e-mail use.

15. Access to certain data sources will be limited (e.g. inappropriate internet sites) in line with our commitment to equality and diversity or to safeguard our IS infrastructure.

16. Inappropriate (as defined by the Computer Misuse Act 1990, as covered in this policy) or excessive IS use is likely to constitute misconduct and be subject to the Disciplinary Policy or criminal proceedings. The following are specifically prohibited:

- Attempting to access information or systems to which you have no right or authority;
- Connecting unauthorised or unlicensed devices or software to IS;
- Receiving or disseminating inappropriate or offensive material.

17. Further advice on this policy can be sought from either corporate IS or departmental HR.

Responsibilities

18. Corporate and Departmental IS staff are responsible for the security of the IS infrastructure and the maintenance of IS equipment.

19. Employees are responsible for the security of the IS equipment they operate (also refer to the Home Working Policy – Employee Handbook Section B5d - where appropriate) and access to systems via their unique user credentials. Employees should, therefore, make themselves familiar with any security policies, procedures or special instructions which relate to the information systems they use.

20. Employees must report any issues that breach this policy, or the related appendices, (including receipt of offensive materials via e-mail) to their line manager immediately.

Monitoring

21. IS use is routinely monitored corporately via the analysis of e-mail traffic, internet sites accessed and telephone records of calls made and received. Information on issues within departments are provided to the Chief Officer to manage, in line with the employee data protection policy and the code of conduct.

22. The content of communication is not routinely monitored across the City of London, however, in specified circumstances such monitoring may be considered appropriate e.g. telephone calls being monitored for training purposes; where serious misuse of IS is suspected; or where potential criminal activity is suspected.

23. The reasons for, and conditions of, overt monitoring of the use of IS by individuals will be set out, in writing, in advance of such monitoring taking place.

24. Covert monitoring will only occur in circumstances where:

- Legislative provision allows for it; or
- Informing the individual would prejudice a criminal investigation or be prejudicial to the interests of the City of London.

Advice must be sought from Director of HR prior to covert monitoring taking place.