Acceptable Use of IT

Table of Contents

Statement of Intent

1. This policy has been developed as part of the City of London Corporation's commitment to provide employment policies that are relevant for a modern workforce in consultation with the Deputy IT Director and the Senior Information Security Officer (SISO).

2. This policy sets out the principles that City Corporation employees (listed in the scope below) are expected to follow when using any IT facilities (e.g. systems, applications, mobile devices, Wi Fi) in the performance of their work duties.

3. The Director of Human Resources will be responsible for the interpretation, advice and management of the policy and procedure on behalf of the City Corporation.

Scope

4. This policy applies to all employees, contractors, suppliers, volunteers, Members, agency and casual workers at the City Corporation. It also includes others who handle or process information on behalf of the City Corporation and may come into contact with our systems and networks, such as (but not limited to) teaching staff in the three City Schools and staff at the City of London Police. Reference to 'employee' in this policy refers to all those in scope as described above.

5. This policy may be supplemented by local usage policies and guides which are intended to act as an extension to this policy.

6. This policy may be reviewed at regular junctures in accordance with legislative changes, changing information risk and evolving technologies.

Purpose

7. The purpose of the policy is to:

    - ensure that all of the City Corporation's IT facilities, applications, systems, networks, platforms, data and equipment are all appropriately protected against loss, misuse or abuse;

    - provide employees with a framework that outlines appropriate use of IT facilities and electronic devices in the performance of their work duties;

    - protect the City Corporation and its customers (residents, businesses, visitors, staff, service users and Members) from information security threats whether internal or external, deliberate or accidental.

General Principles

Security

8. All IT equipment and information systems provided by the City Corporation remain the property of the organisation 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).

9. Employees are responsible for ensuring their unique user credentials and passwords for all work-related information systems, including network access, are kept confidential. This means that they should not be shared with colleagues or written down or left in a non-secure place and must be protected from misuse.

10. Employees must not attempt to use or gain access to another person's password or sign-on codes. While it is advisable that all City Corporation devices are allocated one user per device, it is understood that there are authorised cases where generic or shared sign-on details are permitted for operational reasons.

11. Employees must minimise the possibility of introducing malicious software to the City Corporation's information systems by not opening unreliable or unknown data sources via e-mail or the internet. Employees must not attempt to install or use unlicensed software on City Corporation's devices and equipment.

12. Employees are reminded that in many cases access to web content may be blocked or reconfigured due to necessary security controls as set down by corporate IT security. More information about social media access and use can be found in the relevant appendices and guides.

13. Employees should note that access to systems is subject to change at any time in order to ensure adequate security controls are in place. Any changes to controls and access will be communicated to employees as relevant.

Confidentiality, Data Protection & Data processing

14. Employees are reminded that they are personally responsible for the data in their care.

15. All personal information held on City Corporation systems must be held in accordance with the Corporate Data Protection Policy (see additional links). Employees are responsible for taking all necessary action to keep personal data secure and in accordance with corporate policies and guidance.

16. City Corporation data must be stored on the IT infrastructure and/or approved devices only, and password/passcode protected wherever possible if stored on any removable media (e.g. memory/USB sticks).

17. Any data stored on removable media such as CDs, DVDs, USB sticks must be encrypted wherever practical.

Personal Use

18. Whilst equipment and systems are provided for organisational use, limited and reasonable personal use outside of working hours (i.e. before and after work, during lunch breaks) will be permitted provided it does not negatively impact on service delivery (see also appendices featuring Internet Access and E-mail and Messaging).

19. Personal usage is a privilege which can be withdrawn if abused and employees should be aware that access to websites with specific content (e.g. gambling, gaming) are blocked. Purchases made online using City Corporation servers are made at the employee's own risk.

20. City Corporation systems such as OneDrive, file share and storage should only be used to store personal, work related data. Each employee will be allocated a private file storage area in which to store up to 10MB of personal work-related data only. Under no circumstances should it be used to store unauthorised software or illegal copies of data such as music, films or images. Employees are required to note the specifics set out later in this policy under the Protective Monitoring section.

Inappropriate Use

21. Inappropriate use (as defined by the Computer Misuse Act 1990, as covered in this policy) of City Corporation technology is likely to constitute misconduct and be subject to withdrawal of access, disciplinary action and/or criminal proceedings as relevant. 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 IT;
    - Tampering with IT systems, for example by deliberately introducing viruses or other malware; bypassing, disabling or subverting system controls;
    - Receiving or disseminating inappropriate or offensive material;
    - Displaying, storing, receiving or transmitting images or text which could be considered offensive e.g. material of a sexual, pornographic, paedophilic,

sexist, racist, libellous, threatening, defamatory, or a terrorist nature or likely to bring the City Corporation into disrepute.

22. Communications tools must be operated in line with relevant health & safety principles e.g. Display Screen Usage. Please see the relevant links at the end of this policy.

Responsibilities

23. Employees are reminded that we are all responsible for adopting the appropriate level of security measures in our use of technology and handling of data.

24. Corporate and departmental IT staff are responsible for the security of the IT infrastructure and maintenance of IT equipment.

25. Chief Officers are responsible for ensuring the successful implementation of the policy within their own department.

26. Line managers are responsible for:

    - ensuring the principles of this policy are upheld within their teams;
    - consulting and receiving authorisation from the Director of HR prior to any covert access and/or monitoring taking place;
    - ensuring that employees with access to the Government Connect Secure Extranet (GCSX) or London Public Services Network (LPSN) within their teams read, and comply with, the GCSX/LPSN User Agreement included as Appendix 3 to the Data Protection Policy.
    - It is important to note that if users currently use a gsi-family domain name (gsi.gov.uk, gcsx.gov.uk or gsx.gov.uk) it must be replaced with a government domain like gov.uk by March 2019. Further information is available at https://www.gov.uk/guidance/securing-government-email

27. Employees are responsible for:

    - reading and understanding this policy and other associated policies (i.e. Data Protection, Social Media, etc.);
    - the security of the IT equipment they operate and access to systems via their unique user credentials. Employees should, therefore, make themselves familiar with any available training, security policies, procedures or special instructions which relate to the information systems they use and refer to the Home Working Policy (see Additional Links below);

- reporting any issues that breach this policy, or the related appendices, (including receipt of offensive materials via e-mail) to their line manager immediately;
- completing the mandatory data protection and related training to comply fully with corporate and local guidance.

28. Breaches of this policy may lead to the City Corporation initiating withdrawal of access to City Corporation IT and information, disciplinary action and in serious cases of misconduct may lead to dismissal from the City Corporation and criminal proceedings. Processes for reporting breaches or misuse are covered in the appropriate Appendix.

Protective Monitoring

29. Any information processed on City Corporation systems or stored on City Corporation drives, including personal data, is subject to inspection where relevant to do so. The City Corporation will refer to relevant legislation in such cases, such as that set out in the Interception of Communications Act and by the Information Commissioner.

30. Employees are asked to note that the IT Division routinely monitors data volume, type and internet/e-mail traffic and telephone records where relevant.

31. Inappropriate use of technology will be escalated to the relevant Chief Officer.

32. Where investigation of the content of personal drives is deemed necessary an impact assessment will always be carried out to identify the purpose, benefits, legislative position and impact of such monitoring and investigation. Such instances will be subject to approval from the relevant Chief Officer/s e.g. Director of Information Security and/or Director of HR.

List of appendices

Appendix 1 – Internet Access
Appendix 2 – E-mail & Messaging
Appendix 3 – Remote Mobile Working
Appendix 4 – Sharing Storage Securely
Appendix 5 – Staying Safe Online

Links / Other resources

Service Response Standards

Data Protection Policy

Display Screen Usage.

Home Working Policy

Code of Conduct

Interception of Communications Act 1985

Employment Code of Practice from the Information Commissioner

Use of Personal Email Policy Statement