Security Policy – People

Table of Contents

Statement of intent

1. The City of London Corporation prioritises the security and protection of its employees, other workers, Members, assets, Intellectual Property, Personal Data and Confidential Information. Security awareness is everyone's responsibility, and everyone must comply with the City Corporation security policies and instructions.

2. This policy includes the terms of any security agreements that the City Corporation enters into with customers, government, partner agencies, specific individual requirements and responsibilities within vetted posts and for specific events.

3. This policy is supported by subordinate corporate security procedures and guidance and should be read and operated in conjunction with other relevant City Corporation guidance and advice set out in Links / Other resources.

Scope

4. This policy applies to all City Corporation employees including teaching staff in the three City schools. It also applies to other workers including agency, casual staff, work experience, interns, volunteers, consultants, contractors and those working under a contract for services to the City Corporation.

5. The Director of Human Resources will be responsible for the interpretation, advice and management of these procedures on behalf of the City Corporation. This policy defines the minimum standards which must be followed.

Aims

6. This policy provides a clear statement and an overarching framework for all people security related policies, procedures and guidance.

7. It sets out the City Corporation's security standards and defines the behaviours which must be adhered to in order to protect employees, other workers, visitors, contractors, assets and reputation.

Definitions

8. The following definitions and common terms are:

- **Assets:** include Intellectual Property, Personal Data and Confidential Information

- **Personal Data:** is information relating to a living identifiable individual which must be held and used (processed) in accordance with the United Kingdom General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018.

- **Data Protection Officer ("DPO"):** public authorities are required to have a DPO to advise them on data protection law, monitor compliance and act as liaison with the Information Commissioners Office ("ICO").

- **Confidential Information**: any information that is not in the public domain and is intended to be protected from disclosure (whether it is proprietary in nature or whether by contract, legal protections such as trade secret laws, or other means). Information may be confidential irrespective of whether it is specifically labelled "confidential", "proprietary" or otherwise, or whether it is oral, written, drawn or stored electronically. Alternatively, labelling information "confidential" or "proprietary" or other classification does not automatically make the information Confidential Information. Personal data may or may not be confidential.

- **Employees**: someone who works directly for the City of London Corporation, either on a permanent or fixed-term contract of employment.

- **Workers**: includes agency, casual staff, work experience, interns, volunteers, consultants, contractors and those working under a contract for services.
- **Members**: An elected Member of the Court of Common Council (100 Common Councilmen and 25 Aldermen)
- **Intellectual Property**: intangible property that is the result of creativity, such as designs, patents, copyrights and trademarks.
- **Security Culture**: an environment in which employees, other workers and Members are conscious of security risks, proactively support measures implemented to mitigate those risks, and feel empowered to challenge behaviours which compromise safety and security.
- **Security Personnel**: representatives of the City Corporation Security Teams, and uniformed guard officers contracted by the City Corporation to provide security at City Corporation buildings and events.
- **Security Policies**: together this policy, all other policies procedures and guidance that relate to the security and behaviours of employees, other workers, Members and visitors. It also relates to information and security of IT and policies and procedures in respect of building security.

Responsibilities

Duties of the Town Clerk and Chief Executive:

9. The Town Clerk will ensure that all appropriate mechanisms are in place for this policy to be applied across the City Corporation. The Town Clerk will provide strategic leadership and ensure resources (including people and financial) are in place to discharge this policy and related security policies.

Duties of Heads of Corporate Departments and Directors:

10. Some Directors have specialist and key duties which must be discharged to ensure our Security Policies and arrangements are implemented. For example, the City Surveyor in relation to buildings and security policies and procedures; the Chief Operating Officer is responsible for employee related policies and training, IT security, procurement and contracts; the Chamberlain and Chief Financial Officer for our financial assets.
11. All Chief Officers must ensure that all employees and workers in their departments:

- are aware of the City Corporation's security policies and understand the importance of compliance with them.
- receive regular message through line management to comply with our security policies, to reinforce and embed a positive and proactive security culture.
- complete any required security training.

12. Chief Officers will ensure:

- that premises or buildings comply with the terms of any Building Protective Security Policy and /or guidance that is in place designed to ensure the physical security of our people, assets, intellectual property and confidential information.

  appropriate protocols and instructions are in place for staff who are required to visit clients, customers and/or act in an official capacity on behalf of the City Corporation

- any non-compliance with the security policies within their business or function area is dealt with in an appropriate and timely manner, and reported on the Security Incident Tracker, and in the case of serious breaches via the corporate Security Director to the Security Board.

- appropriate technical and organisational measures are in place to ensure the confidentiality, integrity and security of information, particularly personal data held by their Departments, and that data protection breaches are reported to the Data Protection Officer immediately.

Strategic Director of Security:

13. The Strategic Director of Security will:

- monitor and assess the overarching security environment both externally and internally and its impact on the City Corporation's security culture, policies and practice.
- from time to time revise or direct the revision of the security policies and the issue of new security policies.
- provide guidance on the security policies where appropriate.
- ensure direct training is made available on the security policies as required.

Duties of all Line Managers:

14. Line managers will

- be responsible for ensuring their staff are fully cognisant with all security related instructions.
- will ensure that any issues of non-compliance by a member of their staff, are dealt with in an appropriate and proportionate manner (dependent upon the nature of the non-compliance) in accordance with the Employee Handbook and HR policies.

Duties of all employees and other workers:

15. All employees and other workers are required to:

- cooperate on all matters relating to safety and security whilst on City Corporation business including support of and adherence to all procedures and guidance, and all reasonable instructions. Failure to comply will be treated seriously.
- act in a responsible manner, conducive to the safety and security of themselves, colleagues and visitors to the City Corporation.
- comply with their building security instructions and, where applicable, wear their identification pass as instructed and remove it on departure.
- comply with any reasonable security requests or instructions whilst on City Corporation premises
- comply with local protocols in place if you are required to carry identification for the purposes of visiting clients, customers or representing the City Corporation
- comply with the instructions of site security personnel for building access controls, in the event of an incident, emergency, drill or test, or any matter concerning security.
- ensure that all personal data and confidential information is securely used and stored, in accordance with the Employee Data Protection Policy, and any associated policies and guidelines. Information stored electronically must be secured appropriately for that system in accordance with the Employee Data Protection Policy and any other associated policies and guidance linked at the bottom of this policy.
- report as soon as practicable using the Security Incident Tracker and to a line manager any matters likely to jeopardise the security of our employees, other workers and visitors, or lead to the potential loss of City Corporation assets or information.
- without prejudice to the above, to ensure all data protection breaches are reported to the DPO as soon as they become known. Should an employee discover a personal data breach, they should report the incident to both their department's AIN reps and also the Compliance Team, in the first instance.

The Compliance Team then assess and review the breach and if it is determined to present a high level of risk, the Compliance Team will then report the incident to the DPO.

- ensure that all work undertaken, and data created or held with Government Security Classifications is stored, processed and destroyed in accordance with official guidance.

Links / Other resources

- Code of Conduct
- Data Protection Policy (Employees)
- Employee Screening Policy
- Acceptable Use of IT Policy
- Security Incident Tracker
- City Secure Hub
- City People Employee Self-Service

- Data Breach Reporting Policy