Employee Data Protection Policy

Table of Contents

Statement of Intent

1. The City of London Corporation is committed to all aspects of data protection and takes seriously its duties, and the duties of its employees, under the Data Protection Act 1998 (DPA). This policy sets out how the City Corporation deals with personal data, including personnel files and data subject access requests, and employees' obligations in relation to personal data.

2. The City Corporation recognises that employees have rights in relation to their own personal data processed by the City Corporation, and as employees of the City Corporation they have responsibilities for the personal data of others (i.e. clients, customers and colleagues) which they process in the course of their work.

Scope

3. This policy applies to all employees and workers at the City Corporation, including teaching and support staff in the three City Schools and support staff in the City of London Police. The term 'employee' used in this policy refers to all those in scope as described above. In addition, contractors, volunteers and agency staff at the City Corporation are expected to observe the data protection principles and to comply with the responsibilities set out in paragraphs 16 – 21 below.

4. This policy may be supplemented by local data protection policies for example within Schools and the Barbican Centre where local policies may act as an extension to this policy.

Purpose

5. The purpose of the policy is to:

    - provide employees with a framework that outlines appropriate use of personal data in accordance with the DPA;

    - protect the City Corporation against liability for the actions of its employees.

Definitions

6. Data protection is about the privacy of individuals, and is governed by the DPA 1998, which defines, among others, terms as follows:

    - **"data"** generally means information which are computerised or in a structured hard copy form (although other information held by a public authority may also qualify);

- **“personal data”** data which can identify someone, such as a name, a job title or a photograph, and include opinions and intentions relating to that individual;
- **“processing”** anything that is done with data – just having data amounts to processing;
- **“data controller”** for the purposes of this policy is the City Corporation
- **"data subject"** is an individual who is the subject of personal data.

Data Protection Principles

7. The DPA sets out eight principles governing the processing of personal information, and all these must be fully complied with every time personal data are processed. The principles require that personal data must be:

    - obtained and used fairly and lawfully
    - used for limited, specifically stated purposes
    - adequate, relevant and not excessive for the purpose(s)
    - accurate and kept up-to-date
    - kept for no longer than is absolutely necessary
    - handled according to people’s data protection rights
    - kept safe and secure from unauthorised use
    - not transferred outside the European Economic Area without adequate protection

8. Stronger legal protection applies to more sensitive personal information, such as:

    - Racial or ethnic background
    - political opinions
    - religious beliefs
    - mental or physical health
    - sexual life
    - trade union membership
    - criminal proceedings or records

Responsibilities

The City Corporation

9. As a data controller the City Corporation has publicly registered its general purposes for processing personal data on the Information Commissioner’s website.

10. As part of the purpose of "employee administration" the City Corporation may disclose personal data to professional advisers (e.g. legal or medical), pension

scheme administrators, banks and insurers, and other companies to which the City Corporation has contracted work relating to any of the purposes stated on the register. Information about employees may also be disclosed where required by law, or in connection with legal proceedings, or for the prevention / detection of crime, or assessment / collection of tax. Information about employees may also be disclosed to others at the employee's request or with the employee's consent.

11. Special provisions apply to the processing of sensitive personal data (see para.6), and generally the processing of such information will be avoided where possible. Where the City Corporation needs to process sensitive personal data we will rely on the subject's explicit consent given in the contract of employment, or on one of the other justifications specified under the first principle, or we will seek, if appropriate, the data subject's specific consent

12. The City Corporation operates an Access to Information Network (AIN), consisting of representatives from each department which supports the work of the Information Officer. A list of all AIN Reps at the City of London is available on the Access to Information pages of the Intranet.

13. The Departmental AIN Rep should be the first port of call, when a matter concerning DPA has arisen. If you are unable to contact your AIN Rep, you should contact the Information Officer or Assistant Information Officer.

Managers

14. Managers should ensure that employees:

    - have undertaken the mandatory online training course on DPA
    - are familiar with local procedures and practices regarding the processing of all personal data with which they have access in the course of their duties.

Employees

15. Employees provide explicit consent to the City Corporation to process personal information about them by signing their contract of employment and attention is drawn to the City Corporation's Data Protection Notice to Employees (Appendix 1) advising how data may be processed.

16. Employees are responsible for maintaining their own personal information (i.e. bank details, home address etc.) and can do so through the HR self-service system or by advising the HR Business Unit.

17. Employees with access to and responsibility for personal data are expected to:

    - use data responsibly and in accordance with the data protection principles and should be cautious about disclosing personal data both within and outside

the City Corporation, and about using it in email and via the internet or intranet;

- undertake mandatory DPA and related training comply fully with corporate and local guidance, procedures and practice regarding the processing of personal data and check their authority to take any action involving personal data with their manager;
- report any loss or compromise of own or others personal information to the local Access to Information Network representative as soon as possible;
- take all necessary actions to keep electronic devices secure, in accordance with corporate policies and guidance;
- take all necessary actions to keep personal information in hard copy format secure, in accordance with corporate policies and guidance.

18. Where personal information is to be disposed of, employees should ensure that it is destroyed permanently and securely. This may involve the permanent removal of the information from the server, so that it does not remain in an employee's inbox or Deleted Items folder or Recover Deleted Items folder. Hard copies of personal information may need to be confidentially shredded or placed in confidential waste bins where available. Employees should be careful to ensure that personal information is not disposed of in a wastepaper basket/recycle bin.

19. If an employee acquires any personal data in error by whatever means, they shall inform their AIN representative immediately and, if it is not necessary for them to retain it, destroy the personal data.

20. An employee must not take any personal information away from the City Corporation's premises save in circumstances where prior consent is obtained from their line manager or senior officer.

21. Any employee taking records off site must ensure that appropriate steps are taken to protect it, be it in hard copy, or stored on a laptop or other electronic device. Care must also be taken when observing personal data in hard copy or on-screen so that such information is not viewed by anyone who is not legitimately privy to it.

22. If an employee is in any doubt about what they may or may not do with personal information, they should seek advice from their AIN representative before taking any action.

Accessing Personal Data / Subject Access Requests (SARs)

23. Data subjects have a general right of access (subject to exemptions) to the personal information held about them. This right can be exercised by submitting a Subject Access Request (SAR). A charge of £10 may be applied prior the disclosure of personal data under a SAR.

24. All responses to SARs and disclosure of personal information should be coordinated by the departmental AIN representative in accordance with the Data Protection Subject Access Requests Policy. Departments may issue local guidance in handling this type of request, which act as an extension to the policy.

25. Some personal data may be exempt from disclosure to the data subject, for example:

    - Information about the City Corporation's intentions in relation to negotiations with employees
    - Information to be processed for the purposes of management planning
    - Information that would reveal the identity of another individual, without that individual's consent (but subject to the Information Commissioner's guidelines)
    - Confidential references written by the City Corporation
    - Communications relating to legal advice between the City Corporation and its legal advisers as this is subject to legal professional privilege (a case by case basis);

26. If a data subject thinks that any of their personal information is inaccurate, they will be required to detail what information they want reviewed and why, after which the departmental AIN Representative will be notified.

27. The personal information kept about employees to which access can be given, includes personnel files, sickness records, disciplinary or training records, appraisal or performance review notes, emails in which the employee is the focus of the email and documents that are about the employee.

28. If an employee as the data subject wishes to obtain their personal information (beyond what is held on any corporate HR self-service systems), they should write to the AIN Representative to make a Subject Access Request, specifying the information requested and providing proof of identity. Requests will be acknowledged and, subject to any exemptions or constraints to disclosure under the DPA, the information will be provided within 40 calendar days. It will be explained why the information is being processed and to whom it is disclosed."

29. If an employee becomes aware that the City Corporation holds any inaccurate, irrelevant or out-of-date personal information about them, it may be possible for them to update this themselves (through any corporate self-service HR systems). Where

this is not possible, they should notify the HR business unit and provide any necessary or suggested corrections and/or updates to the information.

30. Any employee receiving a SAR from a data subject directly should immediately pass it to their AIN representative. At the same time, the Information Officer should be informed of the receipt of the SAR. All responses to SARs should be coordinated by the departmental AIN representative, in liaison with the Information Officer, and in accordance with the City Corporation's SARs Policy and Guidance.

31. As part of the on-going move to self-service, address and contact details for a manager's immediate reports are accessible for business purposes.

Data Protection Breaches

32. Failure to observe the data protection principles within this policy may result in an employee incurring personal criminal liability. It may also result in disciplinary action up to and including dismissal.

33. Employees must immediately report to their AIN representative and the Information Officer, any possible breach of the DPA. The breach will be investigated in accordance with corporate procedures.

Monitoring

34. Since the City Corporation's communications facilities are provided for the purposes of the City Corporation's business, employees should not expect that their communications will be private, although the City Corporation will, subject to its overriding business requirements, do its best to respect an employee's privacy and autonomy at work.

35. The City Corporation may monitor an employee's internal and external communications (whether via telephone, email, and internet, or otherwise) for the purposes specified in the Code of Conduct in accordance with the Communications and Information Systems Use Policy.

Training & Compliance

36. The City Corporation provides training to all employees on data protection matters on induction and on a regular basis thereafter. This training is mandatory.

37. The City Corporation will review and ensure compliance with this policy at regular intervals.

List of appendices

Appendix 1 - Data Protection Notice to Employees

Links / Other Resources

Code of Conduct

Communications and Information Systems Use Policy

Corporation of London Data Protection Policy

Data Protection Act 1998

Data Protection (Processing of Sensitive Personal Data) Order 2000

Data Protection Subject Access Requests Policy

Information Commissioner's Office

The City of London and Access to Information

Regulation of Investigatory Powers Act (RIPA) Policy

Regulation of Investigatory Powers Act 2000