Data Protection Policy (Employees)

Table of Contents

Statement of Intent

1. The City of London Corporation (City Corporation) is committed to all aspects of data protection and takes seriously its duties, and the duties of its employees, under the General Data Protection Regulation 2016 (GDPR) and the Data Protection Act 2018 (DPA 2018). This policy sets out how the City Corporation deals with employees' 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.

3. The City Corporation has appointed the Comptroller & City Solicitor as Data Protection Officer, the person with responsibility for advising the organisation in relation to data protection compliance, who can be contacted at information.officer@cityoflondon.gov.uk.

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

Scope

5. This policy applies to all prospective, current and former 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 other workers such as, contractors, agency workers, volunteers, interns, apprentices and those undertaking work experience at the City Corporation are expected to observe the data protection principles and to comply with the responsibilities set out in the paragraphs below.

6. This policy should be read in conjunction with the corporate Data Protection Policy and 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

7. The purpose of the policy is to:

    - provide employees with a framework that outlines appropriate use of personal data in accordance with the GDPR and DPA 2018; and
    - protect the City Corporation against liability for the actions of its employees, other workers, former employees and former other workers.

Definitions

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

    - **“Personal data”** any information that relates to an identified or identifiable living individual. This includes where living individuals can be directly or indirectly identified using information such as a name as well as other identifiers such as unique personal identifiers (e.g. payroll and National Insurance numbers), location data or other online identifiers, as well as physical, physiological, genetic mental, economic, cultural or social identity
    - **“Controller”** the person or organisation responsible for determining the purposes and means of the processing of personal data The City Corporation is the data controller in respect of all personal information that relates to the City Corporation’s business.
    - **“Data Protection Officer” (DPO)** public authorities are required to have a DPO to inform and advise on data protection matters, monitor compliance with data protection legislation and act as liaison with the Information Commissioner’s Office (ICO).
    - **"Data subject"** is the identified or identifiable person to whom the personal data relates.
    - **“Processing”** is defined very broadly and encompasses any action performed on or with personal data, including collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction (that is, the marking of stored data with the aim of limiting its processing in the future, erasure and destruction. In effect, it is any activity involving personal data.
    - **“Processor”** is the person or organisation (a third party) who processes personal data on behalf of the data controller.
    - **"Special categories of personal data"** means personal data which reveals a data subject’s racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic, biometric and health data, and information relating to a data subject’s sex life or sexual orientation.
    - **"Criminal records data"** means information about an individual's criminal convictions and offences, and information relating to criminal allegations and proceedings. To note it is lawful to consider spent convictions for certain types of employment listed as detailed in the Rehabilitation of Offenders Act 1974 (Exceptions) Order 1975.

Data Protection Principles

9. The City Corporation is legally required to comply with the six Data Protection principles when processing personal data. These principles require that personal data:

    i. Shall be processed lawfully, fairly and in a transparent manner in relation to the data subject.
    ii. Shall be collected only for specified, explicit and legitimate purposes; and it must not then be further processed in any manner incompatible with those purposes.
    iii. Shall be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed.
    iv. Shall be accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that data which is inaccurate, having regard to the purposes for which it is processed, is erased or rectified without delay.
    v. Shall not be kept in a form which permits identification of data subjects for longer than is necessary for the purposes for which the data is processed. Personal data may be stored for longer periods provided it is processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes. This is subject to the implementation of appropriate data security measures designed to safeguard the rights and freedoms of data subjects.
    vi. Shall be processed in a manner that ensures its appropriate security. This includes protection against unauthorised or unlawful processing and against accidental loss, destruction or damage.

10. The City Corporation tells individuals the reasons for processing their personal data, how it uses such data and the legal basis for processing in its privacy notices. It will not process personal data of individuals for other incompatible reasons.

11. Stronger legal protection applies in relation to the special categories of personal data information:

    - racial or ethnic origin
    - political opinions
    - religious or philosophical beliefs
    - the processing of genetic data
    - the processing of biometric data in order to uniquely identify a person
    - mental or physical health
    - sexual life and orientation
    - trade union membership

12. There are separate safeguards for personal data relating to criminal convictions and offences, or related security measures.

The City Corporation

13. As a data controller the City Corporation has publicly registered its general purposes for processing personal data on the Information Commissioner's Office (ICO) website.

14. As part of the purpose of "employee administration" the City Corporation may, where necessary for a lawful purpose, disclose personal data to professional advisers (e.g. legal or medical), pension scheme administrators including the LGPS Pensions Board, banks and insurers, and other companies to which the City Corporation has contracted work relating to any of the purposes stated on its register of processing activities.

15. 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.

16. Special provisions apply to the processing of special categories of personal data (see definitions), and generally the processing of such information will be avoided where possible. Where the City Corporation needs to process special categories of personal data it 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 i.e. processed lawfully, fairly and in a transparent manner in relation to individuals; or it will seek if appropriate, the data subject's specific consent. The exceptions to individual consent being when collating statistical data for reporting purposes for the City Corporation to fulfil its contractual, management and legal responsibilities.

17. Departments and institutions are responsible for the personal data they hold and process. Accordingly, the City Corporation operates an Access to Information Network (AIN), consisting of representatives from each department which supports this responsibility and the work of the Information Officer. For a list of all departmental AIN representatives at the City Corporation see Links / Other Resources.

18. The departmental AIN representative should be the first port of call, when a matter concerning data protection compliance has arisen. If you are unable to contact your departmental AIN representative, you should contact the Information Compliance Team in the Comptroller and City Solicitor's Department.

Managers

19. Managers should ensure that:

    - They and their employees have completed the mandatory data protection online training course and any further training as appropriate to their role; and

- They and their employees are familiar with local procedures and practices regarding the processing of all personal data to which they have access in the course of their duties.

CityPeople (HR and payroll system)

20. Where personal data held within the CityPeople system is to be disposed of, it is either deleted or redacted and put beyond business use i.e. no unique identification factors remain.

Employees

21. The City Corporation's Employee Privacy Notice (Appendix 1) sets out how personal data may be processed and the legal basis for doing so. In limited circumstances, the City Corporation may rely on employees' explicit consent for processing; where this is the case consent should be freely given, can be withdrawn and will generally be recorded by the employee's signed agreement.

22. As part of the on-going move to employee self-service, managers can view their immediate reports contact information including emergency contact details (where provided) and employment information integral to staff management. However, employees are responsible for maintaining their own personal information (i.e. bank details, home address etc.) whether through City People employee self-service or any other employee self-service system where applicable. Advice or support in doing so is available from the HR Business Unit at CorporateHRHelpdesk@cityoflondon.gov.uk.

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

    - access only data that they have authority to access and only for authorised purposes;
    - comply at all times with the City Corporation's IT, Security and email use policies; and in particular not use a non-corporation email system for the transmission of personal data;
    - 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;
    - complete mandatory data protection and related training to 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 their own or others personal information to the departmental AIN representative or the Information Compliance Team as soon as possible;

- take all necessary action to keep personal data secure, no matter its form or format, including by the proper management of electronic devices, including mobile devices and computer access; implementing and complying with rules on access to premises and secure electronic and hard copy file storage and destruction, and in accordance with corporate policies and guidance.

24. 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, deleted items folder or recover deleted items folder. Hard copies of personal information must be confidentially shredded or placed in confidential waste bins provided. Employees should be careful to ensure that personal information is not disposed of in a wastepaper basket / recycle bin. It must be remembered that the destruction of personal data is of itself "processing" and must be carried out in accordance with the data protection principles.

25. If an employee acquires any personal data in error by whatever means, they shall inform their departmental AIN representative immediately and, if it is not necessary for them to retain it, destroy the personal data without any further processing of it.

26. An employee must not send other people's personal data from a City Corporation laptop, desktop, tablet or mobile phone to a personal email account i.e. an account not owned or controlled by the City Corporation, except where it is legally permitted to do so.

27. Where employee personal data needs to be taken off site the responsible employee must ensure that appropriate steps are taken to protect it; be it in hard copy, stored on a laptop or other electronic device. For the removal of hard copy information, prior consent should be obtained from their line manager or senior officer. 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.

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

Accessing Personal Data / Subject Access Requests (SARs)

29. Data subjects have a general right of access (subject to exemptions) to the personal data held about them. This right can be exercised by submitting a Subject Access Request (SAR). The type of personal data kept about employees includes personnel files, occupational health and 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.

30. Any employee receiving a SAR from a data subject directly should immediately pass it to their departmental AIN representative and the Information Compliance Team. All responses to SARs should be coordinated by the relevant departmental AIN representative or the Information Compliance Team.

31. Some personal data may be exempt from disclosure to the data subject, but these exemptions or restrictions, are to be assessed on a case by case basis. If a subject access request is manifestly unfounded or excessive, the City Corporation is not obliged to comply with it but can agree to respond where costs are agreed to be met.

32. All SARs must be acknowledged. The City Corporation must respond to a SAR, subject to any exemptions or constraints to disclosure, within one month from the date it is received. In some cases, such as where we process large amounts of the individual's data, we may respond within three months of the date the request is received. The departmental AIN representative will write to the individual within one month of receiving the original request to tell him/her if this is the case.

33. 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 these records themselves (through any corporate employee self-service system). Where this is not possible, they should notify the HR Business Unit at CorporateHRHelpdesk@cityoflondon.gov.uk and provide any necessary or suggested corrections and/or updates to the information. The departmental AIN representative will also be notified.

34. If an employee requests the City Corporation to stop processing data or erase data that is no longer necessary for the purposes of processing on either a temporary or an indefinite basis, they should notify the HR Business Unit at CorporateHRHelpdesk@cityoflondon.gov.uk stating the ground(s) for the request. The departmental AIN Representative will also be notified.

35. However, where the deletion of personal data is approved, and the data is processed by another organisation commissioned on the behalf of the City Corporation, the City Corporation will contact the organisation and inform them of the deletion; unless this proves impossible or involves disproportionate effort. Note: this does not apply in the case of taking up certain staff benefits, where an employee elects to enter into an agreement directly with an external benefits provider, then that provider's own privacy notice should be referred to.

36. In some circumstances it may not be possible to comply with a request for erasure of personal data or to stop processing data. Examples include where processing is required in order to comply with a legal obligation for the performance of a public interest task or exercise of official authority.

37. Complaints regarding the City Corporation's processing of personal data should be addressed to: Complaints Officer, Town Clerk's Department, City of London, PO Box 270, Guildhall, London, EC2P 2EJ, UK; or email: complaints@cityoflondon.gov.uk.

Data Protection Breaches

38. 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 where there are significant or deliberate breaches of this policy, such as accessing employee or customer personal data without authorisation or a legitimate reason to do so.

39. Employees must immediately report to their departmental AIN representative and the Information Compliance Team, any actual or suspected data protection breaches, which will be investigated in accordance with the City Corporation's Data Protection Breach guidelines.

40. If the City Corporation discovers that there has been a breach of employee related personal data that poses a risk to the rights and freedoms of individuals, it is required to report it to the Information Commissioner within 72 hours of discovery. The City Corporation will record all data breaches regardless of their effect.

41. If the breach is likely to result in a high risk to the rights and freedoms of individuals, it will tell affected individuals that there has been a breach and provide them with information about its likely consequences and the mitigation measures it has taken.

42. Where the City Corporation engages third parties to process personal data on its behalf, such parties do so based on written instructions, are under a duty of confidentiality and are obliged to implement appropriate technical and organisational measures to ensure the security of data.

Privacy Impact Assessment (PIA)

43. Some of the processing that the City Corporation carries out may result in risks to privacy. Where processing would result in a high risk to individual's rights and freedoms, the City Corporation will need to carry out a data protection Privacy Impact Assessment (PIA) to determine the necessity and proportionality of the processing. This will include considering the purposes for which the activity is carried out, the risks for individuals and the use of new technologies and the measures that can be put in place to mitigate the risks. Advice should be sought from the Data Protection Officer at an early stage where a proposal may require a PIA.

International Data Transfers

44. Employee related personal data held directly by the City Corporation is not routinely transferred to countries outside the EEA. However, certain data processed by third parties on behalf of the City Corporation may be transferred, for instance organisations based outside the EEA or operating on a global basis may need to transfer or store your personal data outside the EEA. Links to each organisation's privacy notice will be supplied where this occurs.

Monitoring

45. Since the City Corporation's communications facilities i.e. email, messaging, Skype etc. 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.

46. 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

47. The City Corporation provides training to all employees on data protection matters on induction and on a regular basis thereafter. This training is mandatory, and completion of the training will be monitored by Corporate HR and Business Services Unit.

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

List of Appendices

Appendix 1 – Employee Privacy Notice

Links / Other Resources

- Code of Conduct
- Communications and Information Systems Use Policy
- Data Protection Policy
- Information Commissioner's Office (ICO)
- Departmental AIN representatives