August 2019

Information Technology

Director of Information Technology

Version 1.0

Data Protection Policy

Contents

1. Background

1.1. The Data Protection Act (DPA 2018), along with the General Data Protection Regulation (GDPR), came into force on 25th May 2018; and modernises laws that protect the personal information of individuals in the UK.

1.2. The legislation places an ongoing accountability requirement on organisations to demonstrate (and document) that they have considered the privacy risks flowing from their processing of personal data. It also strengthens the requirements for organisations to have adequate and appropriate organisational and technical controls in place to protect privacy.

1.3. In accordance with the GDPR and the Data Protection Act 2018 every data subject has the following rights:

- The right to be informed about how their Personal data is to be used;
- The right of access to their Personal data held by the University and other information;
- The right to rectification if their Personal data is inaccurate or incomplete;
- The right to request the deletion or removal of Personal data where there is no compelling reason for its continued processing;
- The right to restrict processing in certain circumstances;
- The right to data portability which allows individuals to obtain and reuse their Personal data for their own purposes across different services;
- The right to object to processing in certain circumstances;
- Rights in relation to automated decision making and profiling;

1.4. City is a data Controller in terms of the Data Protection Act 2018 and is registered with the Information Commissioners Office (ICO) with the registration number Z8947127.

2. Purpose

2.1. City, University of London (hereafter "City" or "the University") is committed to a policy of protecting the rights and privacy of individuals with regard to its processing of their personal data.

2.2. The purpose of the Data Protection Policy is to:

- Promote the highest standards of information handling practice
- Set out the framework by which City will demonstrate compliance with Data Protection legislation.

3. Normative Reference

3.1 This document forms part of an ISO/IEC27001 aligned ISMS.

4. Terms and Definitions

4.1 For the purpose of this document, the terms and conditions given in ISO/IEC 27001 apply.

4.2 Standard IT terminology is used.

5. Scope and Applicability

5.1. This policy covers the processing of personal data (i.e. data relating to living individuals) where City is a "data controller" or "data processor". (For the definition of these terms, please see Section 13, Definitions, below.)

5.2. The policy applies to all personal data processed by City. This includes, data about:

- current, past and prospective students and members of staff and their family members;
- people who take part in our research;
- contractors and suppliers;
- donors and supporters of the University;
- customers and clients of services and facilities provided by the University;
- visitors to the University.

5.3. The policy applies to all those who carry out data processing for City as a data controller. This includes staff, students, researchers or agents of the University who process personal data on behalf of the University.

5.4. The policy applies to all forms of processing of personal data by City. This includes: (i) any activity involving personal data, such as collecting, analysing, sharing, transferring storing or deleting it)in any media or format; and (ii) electronic personal data, photographic, video or audio personal data, and personal data in the form of human tissue samples, biometric or genomic data and paper records. The policy also applies whether we collect the information from individuals, whether it is provided to us by those individuals or other people or whether it is collected from other sources.

5.5. Additionally, the University requires adherence to the principles of this data protection policy by associated or partner institutions and 3rd parties or in any case where data is shared and processed between the University and other institutions.

5.6. This policy does not apply to processing undertaken by individuals for private ends, even in cases where University equipment is used for such processing.

6. General Policy

6.1. City collects, holds and processes personal data to perform its public task as a university, to pursue its legitimate interests and to discharge certain statutory and regulatory responsibilities.

6.2. City will record and document the legal basis for its processing of personal data. Such processing must have a legal basis and meet at least one of the following conditions:

- Contract: The processing is necessary for a contract City has with the individual, or because they have asked us to take specific steps before entering into a contract.
- Legal obligation: The processing is necessary for City to comply with the law (not including contractual obligations).
- Public task: The processing is necessary for City to perform a task in the public interest or for its official functions, and the task or function has a clear basis in law.
- Legitimate interests: The processing is necessary for City's legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests.
- Consent: The individual has given clear consent for City to process their personal data for a specific purpose.
- Vital interests: The processing is necessary to protect someone's life.

6.3. City will take the following measures in order to meet its obligations under the DPA 2018 and GDPR:

- Taking a 'data protection by design and default' approach;
- Putting written contracts in place with organisations that process personal data on its behalf;
- Maintaining documentation of its processing activities;
- Implementing appropriate security measures;
- Recording and, where necessary, reporting personal data breaches;

- Carrying out data protection impact assessments for uses of personal data that are likely to result in high risk to individuals' interests;
- Adhering to relevant codes of conduct and signing up to certification schemes.

6.4. In processing personal data, City is committed to respecting the privacy rights of individuals and meeting its obligations as a data controller in accordance with all relevant data protection and privacy legislation to which it is subject.

6.5. When processing any personal data, City will always observe the following principles:

a. Lawfulness and fairness:

- Personal data should be processed lawfully, fairly and in a transparent manner. City will be fair and transparent when processing personal data by providing data subjects with the information required to ensure they understand the nature of the processing and how to exercise their rights in relation to that processing.
- For data to be processed transparently, individuals must be given clear and adequate information before their Personal data is collected to enable them to understand how and why their Personal data is to be used so they can take an informed decision about whether or not to provide the data. This is often done using a Privacy Notice. The University has prepared separate privacy notices for the different categories of people the University processes information about, shown on the University website.
- For data to be processed lawfully, one of the legal bases set out in the GDPR (see 6.2 below) must also apply.

b. Purpose Limitation:

- Personal data should be collected for specified, explicit and legitimate purposes.
- Personal data will only be collected for particular purposes which have been made clear to the data subject. It should not be further used or re-used for new or different purposes (unless one of the exceptions in Data Protection Law applies).

c. Data minimisation:

- Personal data processed should be adequate, relevant and limited to what is necessary in relation to the specified purposes for which they are processed.
- Whenever possible, personal data should be anonymised or pseudonymised at the earliest opportunity.

d. Accuracy:

- Personal data processed should be accurate and, where necessary, kept up to date. Schools and services will ensure mechanisms are in place to maintain correct and accurate personal data and to review data exception reports and resolve data errors promptly.
- Staff are reminded of the importance of and requirement to maintain correct and accurate personal data and to review the data exception reports and resolve all data errors promptly.

e. Storage limitation:

- Personal data should be kept in a form which permits identification of individuals for no longer than is necessary for the purposes for which the Personal data are processed.
- When no longer needed for the purpose for which it was collected, and if there is no lawful basis for continuing to keep it, the personal data must be either fully anonymised or securely deleted in accordance with the relevant personal data retention schedule.

f. Security:

- Personal data should be processed in a manner that ensures appropriate security of the Personal data including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.
- City will put in place appropriate organisational and technical controls in order to protect privacy.

6.6. For special category personal data (which is defined in Section 13, Definitions, below), at least one of the following conditions must be met (alongside one of the legal basis described above in paragraph 6.2 above):

- The data subject has given explicit consent;
- The processing is necessary for the purposes of employment, social security and social protection law;
- The processing is necessary to protect someone's vital interests;
- The processing is carried out by a not-for-profit body;
- The processing is manifestly made public by the data subject;
- The processing is necessary for legal claims;

- The processing is necessary for reasons of substantial public interest;
- The processing is necessary for the purposes of medicine, the provision of health or social care or treatment or the management of health or social care systems and services;
- The processing is necessary for public health;
- The processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to certain safeguards.

7. Personal data security

7.1. City will put in place appropriate organisational and technical controls in order to protect privacy. Such controls will include:

- Undertaking appraisals and assessments of new projects, proposals and initiatives (including research) that relate to the processing of personal data;
- Adoption of the City DPIA issued in June 2019 which provides a best practice framework;
- Ensuring that personal data held in physical records is identified, documented and appropriately secured and controlled.
- Putting in place appropriate authentication schemes to ensure the 'confidentiality, integrity and availability' of systems and services and the personal data processed within them;
- Ensuring that personal data is only stored and processed on City University London supplied and/or approved IT systems and 3rd party services;
- Ensuring that encryption and/or pseudonymisation is used where it is appropriate to do so.
- Assessing and recording the information security posture of suppliers of systems and services that will be used to store or process personal data prior to contract.
- Maintaining mechanisms for the secure and confidential destruction of physical records and disposal of electronic storage media.

7.2. City will not transfer personal data to a state that is not a member of the European Union unless the recipient processor has in place adequate measures to safeguard the privacy rights of data subjects.

7.3. Personal or unapproved systems/services/storage devices (eg. Personal USB sticks/hard drives, Cloud storage services, Google Documents, Dropbox, Gmail etc.) must not contain personal data where City is a "data controller" or "data processor".

8. Personal data breach reporting

8.1. A personal data breach is an incident that affects the confidentiality, integrity or availability of personal data. A breach will occur where there is accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to, personal data.

8.2. It is important that personal data breaches are identified and reported as soon as possible. Some types of personal data breach must be reported to the Information Commissioner's Office within 72 hours: If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, organisations must also inform those individuals without undue delay.

8.3. Should a data breach occur, it is extremely important to ensure that it is dealt with immediately and appropriately to minimise the impact of the breach and to help prevent any recurrence. Staff should report any breach or suspected breach to the IT Service Desk.

8.4. The university will maintain records of personal data breaches and investigations.

9. Access to personal data

9.1. Individuals have the right of access to their Personal data held by the University. An individual is only entitled to their own personal data, and not to information relating to other people (unless they are authorised to act on behalf of someone).

9.2. Requests from individuals for their own personal data will be handled as Subject Access Requests. Such requests should be logged with Dataprotection@city.ac.uk for processing.

9.3. Where a request for personal information is received from a third party, the lawful basis of the request, the impact of disclosure on the data subject and the prejudice to the public interest of withholding the information will be carefully considered before a decision is made on to whether or not to release it.

9.4. Sharing of personal data with third parties for business or research purposes will require the University to put appropriate contracts and/or agreements in place.

10. Roles and Responsibilities

Data Protection Officer

10.1. City will appoint a Data Protection Officer, to conform to the requirements of the Data Protection Act 2018 and the GDPR to carry out the following statutorily defined tasks:

- to inform and advise City and its staff about the need to comply with data protection and privacy legislation and this Policy;
- to monitor the City's compliance with data protection and privacy legislation and this Policy;
- to raise awareness of data protection and privacy issues;
- to ensure that adequate training is undertaken by the City's staff in respect of data protection and privacy;
- to conduct internal audits of compliance
- to advise on, and to monitor, data protection impact assessments (DPIA); and
- to be the first point of contact for the Information Commissioner and to cooperate in the same
- coordinate the City's responses to enquiries from data subjects about data protection and their privacy rights.

10.2. The Data Protection Act 2018 requires that the Data Protection Officer, reporting directly to the highest level of management, shall enjoy the independence necessary to perform their tasks and shall be sufficiently well resourced; and will suffer no penalty as a result of performing their tasks.

Information Governance Committee

10.3. An Information Governance Committee chaired by the Chief Financial Officer will oversee City's compliance as an organization with the Data Protection Act 2018 and General Data Protection Regulation (GDPR).

10.4. The Information Governance Committee will make sure that City evidences the steps it takes to comply and will review and update its accountability measures at appropriate intervals.

Senior Information Risk Owner (SIROs) responsibilities

10.5. SIRO's will be appointed by each School at City and each Professional service; and will be responsible for protecting and defending school / departmental information by ensuring its confidentiality, integrity and availability. This involves:

- Acting as the data controller in relation to the Information Assets used by the school / department;
- Promoting a 'data protection by design and default' approach when considering new or changes to existing personal information handling processes and practices;
- Ensuring Information Asset Owners maintain up to date records of Information Assets and processing activities;
- Identifying, evaluating and managing departmental information risks;
- Ensuring that appropriate control, agreements or contracts are in place to govern the access to, and sharing of, information assets held by the department;
- Maintaining departmental records management arrangements and applying retention policies;
- Maintaining oversight of breaches and security incidents and ensuring remediation and following actions are implemented promptly;
- Reporting on the effectiveness of departmental information handling arrangements to the Data Protection Officer.

Information Asset Owners & Administrators

10.6. Information Asset Owners & Administrators will be appointed for each Information Asset owned by City and will record and maintain records of processing personal data in an Information Asset Register. The register will record, as a minimum,

- The purposes of the University's processing;
- A description of the categories of individuals and categories of personal data;
- The categories of recipients of personal data;
- Details of transfers of personal data to third countries including documenting the transfer mechanism safeguards in place,
- Retention schedules,
- A description of the technical and organisational security measures in place to protect individual's privacy.

Managers and staff

10.7. Managers and all staff who process personal data on behalf of City have a responsibility for ensuring that data protection issues within their areas are managed in a way that meets the provisions of this policy and that all staff undertake the mandatory training necessary to fulfil that role.

10.8. City expects all staff to process personal data for which City is controller or processor in accordance with this policy and that the principles set out above are observed.

Students

10.9. City expects all students to process personal data for which City is controller or processor in accordance with this policy and that the principles set out above are observed.

11. Training and awareness

11.1. City will ensure there is a good level of understanding and awareness of data protection amongst its staff. This will be achieved through the provision of:

a. An on-line suite of guidance materials;

b. An auditable computer-based training solution for all staff covering the fundamentals of data protection, GDPR and information security awareness;

c. Tailored training for SIROs, Information Asset Owners/Administrators and staff regularly involved in high risk processing of personal information.

11.2. It will be mandatory for all staff to complete computer-based training on the fundamentals of data protection, GDPR and information security awareness;

12. Compliance

12.1 Compliance Measurement

The Information Security team will verify compliance to this policy through various methods, including but not limited to, periodic walk-through's, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

12.2 Exceptions

Any exception to the policy must be approved by ExCo in advance.

12.3 Non-Compliance

Any reckless or wilful conduct by staff or students which undermines this Policy or puts at risk the security of any personal data may result in disciplinary action being taken against them. All such cases will be fully investigated according to the University's Disciplinary Procedures and may be reported to the ICO.

In the case of a criminal offence City will involve the appropriate authority.

13. Definitions

Data Protection and Privacy Legislation	This includes the Data Protection Act (hereafter "DPA"), the General Data Protection Regulation (hereafter "GDPR") and the Privacy and Electronic Communications Regulations (hereafter "PECR"), as well as other future legislation that supplements or supersedes the aforementioned.
Personal data	Any data or information or any combination of data relating to an identifiable living person who can be directly or indirectly identified in particular by reference to an identifier. These identifiers can include a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person.
Special category data	Special Category data, sometimes referred to as 'special character data' is personal data which is particularly sensitive and requires an enhanced level of protection. Examples of special category data include: Racial or ethnic origin, Medical history, Political opinions, Religious or ethical beliefs, Trade union membership, Genetic or Biometric data, Sexual Orientation and Criminal history
Data Subject	An identifiable living person who can be identified, directly or indirectly from Personal data.
Processing	Processing occurs when City treats personal data in any way, whether or not by automated means. Examples of processing are collection, storage, disclosure, review and erasure.
Data Controller	An organisation which determines the purposes and means of processing Personal data.
Data Processor	An organisation or person which is responsible for processing personal data on behalf of a Data Controller.
Personal data breach	A breach is a security incident that affects the confidentiality, integrity or availability of personal data. A breach will occur where there is accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to, personal data.
Information Commissioner's Office	The Information Commissioner's Office is the UK's independent authority set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals.

14. Risk Management

Risk management for each department is defined within their Risk Management Policy.

15. Policy Review

This policy will be reviewed by the process owner and updated alongside the security operating procedures on a regular basis, not to exceed 12 months.