Data Protection Policy

Version	2.0
Status	Approved, January 2023
Owner/Author	Information Assurance
Approved by	Information Governance & Security Committee
Approval date	18 January 2023
Review date	January 2024

Contents

1.0 Purpose and Scope

City is a data controller in terms of the DPA 2018 and is registered with the Information Commissioner's Office (ICO) with the registration number Z8947127.

This policy provides a framework for ensuring that the City, University of London, meets its obligations under the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA 2018), as well as other related legislation (the data protection legislation).

This policy applies to all types of personal data processed by, or on behalf of City, and to all people or organisations who process personal data on behalf of City, including staff, students, joint controllers, contractors and processors.

The policy 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.

City hosts information for Students' Union and trade union activities, as well as information processed by individuals for private ends, including in staff, student and alumni email accounts. Please note that where City does not determine the means and purpose of personal data processing, and it is not acting on behalf of another data controller, it is not a data controller or a data processor of the information being processed, even if the processing takes place on City systems or platforms.

City complies with the data protection legislation guided by the six data protection principles.

In summary, they require that personal data is:

- processed fairly, lawfully and in a transparent manner.
- used only for limited, specified stated purposes and not used or disclosed in any way incompatible with those purposes.
- adequate, relevant, and limited to what is necessary.
- accurate and, where necessary, up to date.
- not kept for longer than necessary; and
- kept safe and secure.

In addition, the accountability principle requires us to be able to evidence our compliance with the above six principles and make sure that we do not put individuals at risk because of processing their personal data.

Failure to do so, can result in breach of legislation, reputational damage, or financial implications due to fines. To meet our obligations, we put in place appropriate and effective measures to make sure we comply with data protection law. Our staff have access to a number of policies, operational procedures and guidance to give them appropriate direction on the application of the data protection legislation, this includes:

- Acceptable Use Policy
- CCTV Policy
- Conditions of Use Policy
- Information Security Policy
- Guidance on Safe Data Handling and Storing and Sharing Data.

2.0 Normative Reference

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

3.0 Terms and Definitions

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

3.2 Standard IT terminology is used.

4.0 Information covered by Data Protection Legislation

The UK GDPR definition of "personal data" includes any information relating to an identified or identifiable natural living person.

Pseudonymised personal data is covered by the legislation, however anonymised data is not regulated by the UK GDPR or DPA 2018, providing the anonymisation has not been done in a reversible way.

Some personal data, known as special category data, is more sensitive and is afforded more protection. This is information related to:

• Race or ethnic origin;
• Political opinions;
• Religious or philosophical beliefs;
• Trade union membership;
• Genetic data;
• Biometric ID data;

• Health data;
• Sexual life and/or sexual orientation; and
• Criminal data (convictions and offences).

5.0 Our Commitment

City is committed to transparent, lawful, and fair proportionate processing of personal data. This includes all personal data we process about students, staff, alumni or those who work or interact with us.

- Information Asset Owners: we assign an Information Asset Owner (IAO) to each information asset throughout the organisation, who together with a network of teams and staff with information management responsibilities aid City in managing personal data and its associated risks.

- Privacy Notices: we publish general, student, staff and alumni privacy notices on our website and provide timely notices where required.

- Training and awareness: we make mandatory data protection available for staff to re-take every two years. Additional training and resources are made available. City will ensure there is a good level of understanding and awareness of data protection amongst its staff.

- Breaches: we consider personal data breach incidents and have a reporting mechanism that is communicated to all staff. We assess whether we need to report breaches to the ICO as the Regulator of DPA 2018. We take appropriate action to make data subjects aware if needed. We keep records of data breaches and near misses.

- Information Rights: we have a dedicated team and clear processes to handle subject access requests and other information rights requests.

- Data Protection by Design and Default: we have a procedure to assess processing of personal data perceived to be high risk, that needs a Data Protection Impact Assessment (DPIA) carried out, and processes to assist staff in ensuring compliance and privacy by design is integral part to any product, project or service we offer.

- Records of Processing Activities (RoPAs): we record our processing activities.

- Policies and Procedures: we produce policies and guidance on information management and compliance that we communicate to staff.

- Communications: we seek to embed a culture of privacy and risk orientation.

- Contracts: our Procurement, Research Contract Management and Information Assurance Teams review contracts to oversee that they are compliant with UK GDPR.

- Data sharing with third parties: this will take place in accordance with the data protection legislation, including where data may be transferred outside of the UK.

- Lawful basis for processing: City documents the lawful bases for processing personal data and, if applicable, the conditions for the processing of special category personal data.

- Security: City implements appropriate organisational and technical controls, including security measures, for the processing of personal data. Personal data for which City is a data controller or data processor will be stored in accordance with City's guidance on safe data handling and storing and sharing.

6.0 Roles and Responsibilities

We have an established framework that supports the identification and management of the risk to personal data across City.

The framework's detailed roles and responsibilities comprises:

6.1 Senior Information Risk Owner (SIRO)

The SIRO owns the overall risk arising from the City's processing of personal data. Our SIRO is City's Chief Operating Officer, Helen Watson, who chairs the IGSC.

6.2 Data Protection Officer (DPO)

The Data Protection Officer (DPO) is primarily responsible for advising on and assessing our compliance with the DPA 2018 and UK GDPR and making recommendations to improve compliance. City's DPO is Emma White, and she can be contacted at dataprotection@city.ac.uk. City's DPO is a member of the IGSC and leads the Information Assurance Team (IAT).

6.3 Information Governance & Security Committee (IGSC)

The IGSC is responsible for the overview and scrutiny of information governance (IG) arrangements and for making recommendations to the Senior Information Risk Owner (SIRO) on information governance with data protection and compliance decisions. IGSC reports to the Senior Leadership Team (SLT) and City's Audit and Risk Committee.

6.4 Information Assurance Team (IAT)

The IAT advises on compliance with data protection, handles information rights requests and freedom of information requests and manages the DPIA review process. It supports the implementation of IT and other solutions to ensure City takes a privacy by design approach. It investigates data breaches and develops training and guidance. The IAT is led by Emma White.

6.5 Information Security Manager

City's Information Security Manager, Mike Cann, reports to the Director of IT and is responsible for IT actions such as technical assessment of third-party suppliers' compliance, the management of security exception requests, technical IT security of systems and technical security policies. He works alongside but independently of the IAT.

7.0 Monitoring

Compliance with this policy will be monitored via the DPO and the responsible teams and persons reporting to IGSC.

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 City's disciplinary procedures and may be reported to the ICO.

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

8.0 Risk Management

The IGSC will maintain a risk register which will be reviewed on a regular basis, at least every 12 months.

9.0 Policy Review

This policy will be reviewed by the process owner and updated on a regular basis, at least every 12 months.

10.0 Further information

Our corporate standards and policies are available via the following links:

General Privacy Notice
Student Privacy Notice
Staff Privacy Notice
Alumni Privacy Notice
Policies
Information rights requests

11.0 Glossary

- Data controller: the organisation (or individual) which, either alone or jointly with another organisation (or individual) decides why and how to process personal data. The Controller is responsible for compliance with the DPA 2018 and UK GDPR.

- Data processor: an organisation or person which is responsible for processing personal data on behalf of a data controller.

- Data protection legislation: this includes the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA 2018), as well as the Privacy and Electronic Communications Regulations 2003 (PECR), the Freedom of Information Act 2000 (FOIA 2000) and the Environmental Information Regulations 2004 (EIR 2004), and other (future) legislation that supplements or supersedes the aforementioned.

- Data subject: an identifiable living person who can be identified, directly or indirectly from personal data.

- Information Commissioner's Office (ICO): the ICO 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.

- Personal data: any information relating to an identifiable living individual who can be identified from that data or from that data and other data. This includes not just being identified by name but also by any other identifier such as ID number, location data or

online identifier, or being singled out by any factors specific to the physical, physiological, genetic, mental, cultural or social identity of the individual.

- Personal data breach: a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored, or otherwise processed.

- Processing: anything that is done with personal data, including collection, storage, use, disclosure, and deletion.

- Pseudonymisation: the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.

- Special category personal data: personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying an individual, data concerning health or data concerning an individual's sex life or sexual orientation.