February 2017
Information Technology
Director of IT

Data Protection Policy

1. City, University of London (hereafter “the University”) is committed to a policy of protecting the rights and privacy of individuals with regard to the processing of their personal data.

Scope

2. This policy covers the processing of personal data (i.e. information about living individuals) whose use is controlled by the University and defined in the University’s Data Protection Notification. It applies to any staff, students, researchers or agents of the University who process personal data on behalf of the University. The University should continue to require adherence to the principles of this data protection policy by associated or partner institutions in any case where data is shared between the University and another institutions.
3. Personal data applies to both computer and manual records, including filing systems and micro fiche records.
4. This policy does not apply to processing undertaken by individuals for private ends, even in cases where University equipment is used for such processing.
5. In addition various codes of conduct, guidance and best practice notes relating to specific area will also be published.
6. This policy, and its subsidiaries, shall be reviewed and updated annually to ensure that they remain appropriate in the light of any relevant changes to the law, organisational policies or contractual obligations by the Information Services Management Team. Additional regulations may be created to cover specific areas as required.

Objectives

7. The University seeks to ensure that all processing of personal data carried out on its behalf will comply with the requirements of the Data Protection Act, 1998 (hereafter "the Act"), including the eight principles of good practice laid out in Schedule 1 of the Act. To these ends, the University seeks in particular to ensure that all those processing data on their behalf are aware of their obligations in processing data under the Act and that data subjects are made aware of their rights, as laid out in the Act, which must be respected by the University.

Notification

8. The University undertakes to maintain an accurate and timely notification of its data processing activities with the Information Commissioner's Office (ICO), which shall be available on request to data subjects at: www.ico.org.uk/what_we_cover/register_of_data_controllers. Maintenance of the notification is the responsibility of the Information Compliance Officer. Staff must be made aware that, in cases where they undertake new processing, they must inform the Information Compliance Officer, so that the University notification can be reviewed.

9. The University reserves the right to audit data processing being undertaken in any of its constituent departments, to ensure that processing is legitimate and that the University notification remains valid. The initiation of such and audit will be the responsibility of the Chief Information Officer.

Fair Obtaining and Processing

10. In line with the requirements of Principle 1 of the Act (fair processing, the University undertakes to ensure that whenever data subjects submit information; they are clearly informed about the uses of that information (fair processing notice) and (where relevant) they give their informed consent for processing. These requirements will be enforced whatever the means of collection. All collection media **must** carry clear statements regarding the processing.

11. Sensitive data shall only be collected for certain specified purposes, and shall be obtained with consent. The University will keep the collection and processing of sensitive data to a minimum.

12. Where sensitive data are disclosed, the conditions include: that the subject's explicit consent has been obtained; or disclosure answers a legal obligation in connection with employment; or disclosure is necessary to protect the subject's vital interests; or the information disclosed as already been put in the public domain by the actions of the data subject; or disclosure is in relation to any legal proceedings; or disclosure is in connection with the monitoring of equality of opportunity.

Information Security

13. The University is committed to information security, and will make every effort to safeguard against inappropriate disclosure of personal information. Please refer to the University's Information Security and Laptop Encryption policies.

Disclosure of Personal Data to Third Parties

14. Where a request for personal information is received from a third party, the identity of that third party and the need for the information must be established before disclosure is even considered. External disclosures of student data should be made only by the Student Registry, except in the cases of academic references. External disclosure of staff data should be made only by the Human Resources Department. Disclosure to the Police may be made by these departments in cases where the Police are pursuing a criminal investigation, but only on receipt of the appropriate form.

Staff and Student Responsibilities

15. The University seeks to ensure that all staff are fully informed of their responsibilities under the Act. All staff should complete the online information security training and attend the Data Protection Act/Freedom Information Act workshop. Details of courses are available on the HR intranet. Appropriate disciplinary action, possibly leading to dismissal, will be taken in cases where a member of staff has committed a clear, willful breach of the Data Protection Act's requirements.
16. It shall be the responsibility of the Information Compliance Officers to ensure that procedures are in place to inform staff of their responsibilities. Staff should been made aware that, in line with the University's policy on open records, and in compliance with the Act, any data (including references, examination reports, emails etc.) which they contribute, in the form of facts or opinions about an individual, may be made available to the individual on request.
17. All staff should have access to a copy of this policy and be made aware of the implications of the Act in relation to their duties. Staff should be made aware that any breach of the Act may represent a criminal offence for which they are personally liable.
18. The University seeks also to ensure that all staff are made fully aware of their own rights as data subjects.
19. Students who need to process personal data as a justifiable part of their studies (whatever the level or mode) will be covered by the University's Data Protection notification. Any student who processes personal data as part of their studies will be supplied with relevant guidance on the data protection regulations and shall

work under the direct supervision of a member of staff.

20. Students who need to process personal data as part of an elected role defined by the University constitution (e.g.as returning officer) shall be supplied with relevant guidance on data protection regulations. The University will take responsibility for destroying electoral lists once they have been used. Students in receipt of data will be warned that the University will take disciplinary action against any student who misuses any data provided.

Research

21. Staff (and, where relevant, students) undertaking research will be covered by the University's Data Protection notification. So long as any research undertaken does not support measures taken against individuals and is not published in a way that would identify individuals or cause them damage or distress, data used for research purposes will enjoy certain exemptions from the terms of the Act. Notably, data may be used for research even if it was not originally collected for that purpose, it may be kept indefinitely, and subjects do not have the right to access the data. Further guidance on the use of personal data for research purposes is provided on the Information Compliance section of the staff intranet.
22. Despite the terms of these exemptions, the University seeks to ensure that, wherever practically possible, data subjects are made fully aware of any research use their data may be put to. Wherever possible, research data will be anonymised before use. Additionally, researchers are required to keep their data secure and to guard against any accidental disclosure that might arise from direct or indirect reference to individuals in any research report.
23. In cases where sensitive personal data (such as NHS data) is being processed, researchers shall need to get the approval through the appropriate University Research Ethics Committee before commencing processing. The Research Ethics Committee will check that appropriate controls are in place regarding data storage, transfer and use. In cases where research data is to be shared with other researchers based overseas, the explicit consent of the research subjects shall be sought.

Subject Access Requests

24. The University undertakes to honour the rights of all data subjects (including students and staff) as laid out in the Act, and will respond in good time to any Subject Access Request so long as the enquirer has submitted the appropriate fee and provided confirmation of their identity.
25. The University seeks to ensure that no data processing undertaken will cause unwarranted damage or distress to data subjects.

26. The University will correct or erase (as appropriate) any data that is found to be incorrect, and (where practicable) will inform all relevant parties of any corrections made to personal data.

27. The University undertakes to discontinue direct marketing to any data subject who specifically requests that they do not wish to receive such communications, even in cases where the subject had previously given consent.

28. The University undertakes to ensure that any decision reached by automated means (for example, a mark given to an exam scripts using optical mark reader technology) will be subject to manual review at the request of any relevant data subject. It will be the responsibility of the relevant Head of Department to ensure that such reviews are conducted thoroughly and in good time (within 21 days of receipt of the request).

Mechanism for Subject Access Requests

29. The University undertakes to co-operate as fully as is reasonable with any Subject Access Request. However, the University reserves the right to refuse to comply with repetitious subject access requests where a reasonable time has not elapsed between the previous and current request.

30. All Subject Access Requests must be routed via the University's Information Compliance Officer – staff in receipt of a request or a potential request should contact the Information Compliance Officer immediately. Subject Access Requests should be made in writing. The University has produced a form for this purpose, which can be found in the Legal section of the University's website. Once the appropriate fee (as determined by the Information Commissioner's Office) and proof of the enquirer's identity and entitlement to the information has been received, a standard search for data will be initiated against a pre-defined set of likely data holders. However, subjects will be permitted, additionally, to specify any other potential data holders whose records should be searched. In any case where data is not supplied (for example, when this would challenge the data protection rights of some other third party) then the enquirer will be informed in writing of the reasons for the non-disclosure.

31. Responses to Subject Access Requests will be provided in a permanent form unless it is believed that this would involve disproportionate effort or the data subject agrees otherwise. Any codes shown shall be translated or explained to the data subject.

32. In all cases, if there is any doubt as to the validity of the enquirer or their enquiry, no disclosure should be made. Persistent callers should be directed to the University's Information Compliance Officer.

Data Accuracy

33. In line with the requirements of Principle 4 of the Act, the University seeks to

ensure that all personal data held is accurate and timely. Data will be reviewed periodically and, where practical and appropriate, the University will provide subjects with copies of data holdings so that inaccurate or out-of-date information may be identified and removed or updated.

34. Data subjects have a responsibility to ensure that they inform the University of any changes to their details.

ICO Assessment

35. The University will co-operate with any Data Protection assessment instigated by the Information Commissioner's Office (ICO). Members of staff will be expected to assist with any assessment.

CCTV

36. The University operates a CCTV monitoring system around its properties. The function of this system is to assist in the detection and deterrence of crime, to assist in traffic management, and to assist the Police and civil authorities in the event of a major emergency. The system will be operated in such a way as to safeguard individuals' right to privacy.

37. All CCTV images have ownership and copyright vested in City, University of London. Consent to use or reproduce material held by the University resulting from the CCTV system will normally be withheld.

38. Individuals may request in writing that they see a recording they believe may hold images of them. This request should be made through the standard Subject Access Request procedure.

Storage and processing

39. Data owned by City, University of London must only be stored or processed on City University London supplied and/or approved IT systems and 3rd party services. Personal or unapproved systems/services/storage devices (eg. Personal USB sticks/hard drives, Cloud storage services, Google Documents, Dropbox, Gmail etc.) must not contain University data. The IT Service Desk can advise with regard to approved/supported systems and services.