Data Protection Policy
Contents

1

Contents ............................................................................................................................................................... 2
Document Control ................................................................................................................................................. 3
Introduction .......................................................................................................................................................... 4
Scope ................................................................................................................................................................... 4
Objectives ............................................................................................................................................................ 4
Legislation and other policy ................................................................................................................................. 4
Application of this policy / Staff responsibility ................................................................................................... 5
Notification .......................................................................................................................................................... 5
Fair obtaining and processing .............................................................................................................................. 5
Data accuracy ....................................................................................................................................................... 6
OIC Assessment ................................................................................................................................................... 6
Subject rights ....................................................................................................................................................... 6
Mechanism for Subject access requests ............................................................................................................... 6
Security: General ................................................................................................................................................. 7
Security: Dealing with third party enquirers ......................................................................................................... 7
Students who process personal data ..................................................................................................................... 8
Research .............................................................................................................................................................. 8
References ............................................................................................................................................................. 9
Examination marks ............................................................................................................................................... 9
Web.................................................................................................................................................................... 9
CCTV ................................................................................................................................................................. 10
Implementation & Guidance .............................................................................................................................. 10
Appendix 1: Glossary of terms ............................................................................................................................... 11
Appendix 2: The Eight Principles .......................................................................................................................... 12
Document Control

Version: Draft 1.4
Date: 19th January 2004
Author(s): Andrew Kinglake
Distribution: All City University Staff & Students (via website)
Review Date: January 2005
Introduction

City University is committed to protecting the rights of individuals’ privacy with regard to the processing of personal data. It has established the following policy to support this commitment. This Policy is based largely on work undertaken at Lancaster University.

The Policy should be read in conjunction with the procedural guidance which can be found at www.city.ac.uk/ic.

Scope

This policy covers the processing of personal data (i.e. information about living individuals) whose use is controlled by the City University and defined in the University’s Data Protection Notification (Z7142657). It applies to any staff, students, researchers or agents of the University who process personal data on behalf of the University. Personal data applies to both computer and manual records, including filing systems and fiche records.

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

Objectives

City University (hereafter “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 new Act and that data subjects are made aware of their rights, as laid out in the Act, which must be respected by the University.

Legislation and other policy

This Policy is to be read in the context of the following legislation:

- Data Protection Act, 1998
- Freedom of Information Act, 2000
- Human Rights Act, 1998

Elements of this policy will also be reflected in, or be informed by, the following other University policies:

- Information Security Policy
- Policy on References
Application of this policy / Staff responsibility

The University seeks to ensure that all staff are fully informed of their responsibilities under the Act. Appropriate disciplinary action, possibly leading to dismissal, will be taken in cases where a member of staff has committed a clear, wilful breach of the Act’s requirements.

It shall be the responsibility of the University Head of Information Compliance & Policy 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.

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.

The University seeks also to ensure that all staff are made fully aware of their own rights as data subjects.

Notification

The University undertakes to maintain an accurate and timely notification of its data processing activities with the Office of the Information Commissioner (OIC), which shall be available on request to data subjects. Maintenance of the notification is the responsibility of the Head of Information Compliance & Policy. Staff must be made aware that, in cases where they undertake new processing, they must inform the Head of Information Compliance & Policy so that the University notification can be reviewed.

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 Director for Information

Fair obtaining and processing

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 (whether paper forms, email, surface mail correspondence, web data collection forms, or any other medium). All collection media must carry clear statements regarding likely processing.

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, and will only process sensitive data for the purposes described in Appendix 3.
Data accuracy

In line with the requirements of Principle 4, 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 regularly will provide subjects with copies of data holdings so that inaccurate or out-of-date information may be identified and eradicated or updated.

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

OIC Assessment

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

Subject rights

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.

The University seeks to ensure that no data processing undertaken will cause unwarranted damage or distress to data subjects.

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.

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.

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

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.

All Subject Access Requests must be routed via the University’s Head of Information Compliance & Policy – staff in receipt of a request or a potential request should contact the Head of Information Compliance & Policy immediately. The Head of Information Compliance & Policy will conduct a
Subject Access Request only on receipt of the appropriate fee (as determined by the Office of the Information Commissioner) and proof of the enquirer’s identity and entitlement to the information. The request should be made in writing. The University has produced a form for this purpose. Once initiated, a standard search for data will be conducted 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.

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.

**Security: General**

The University is committed to holding data in secure conditions, and will make every effort to safeguard against accidental loss and corruption of data.

All staff have a responsibility to keep data securely. Appropriate measures must be taken to ensure that there is no unauthorised access to areas in which records are held. Storage areas that are unattended should be locked, as should offices. Filing cabinets should be locked when unattended. Personal files should be kept away from the public gaze and, where possible, staff should operate a ‘clear desk’ policy. When manual records are no longer required they should be disposed of securely via the University’s ‘confidential waste’ arrangement.

All computer ‘personal record’ systems should be backed up regularly to ensure against loss of data, and PCs should be virus-protected. Access to records systems will be by password only, and staff may not share passwords or log in as some other user. Passwords should be changed on a regular basis. Access to any centrally maintained records system can be authorised only by the relevant systems administrator. Visual Display Units should not be visible to unauthorised people, and should be guarded with password-protected screen-savers where possible. When PCs are recycled for use elsewhere or taken out of service, they should be degaussed or have their hard drives overwritten to US Department of Defense standards before reuse or disposal. Greater detail can be found in the Information Security Policy.

Any member of staff who processes personal data on a laptop that they use beyond the confines of the University campus will be responsible for the safe keeping of that data and that equipment. If travelling, the laptop should be kept in view, or secured in locked luggage.

All departments must seek to ensure that student information is not placed accidentally in the public domain. Departments should publish results – if at all – using student identity number not name. The identity of any student who enquires about their own records (e.g. examination marks) should be verified using the Student Registration number.

**Security: Dealing with third party enquirers**

The University is committed to data security, and will make every effort to safeguard against illegitimate disclosure of personal information.
Internal data transfers made between different departments of the University should be made on an operational basis only. Disclosures to third parties shall be made only where at least one of the ‘conditions for fair processing’ (Principle 1) have been met. These conditions are: that the subject’s consent has been obtained; or disclosure is necessary in relation to a contract to which the subject is a party; or disclosure is in compliance with a legal obligation placed on the University; or disclosure is necessary to protect the subject’s vital interests; or disclosure is necessary for the purposes of legitimate interests pursued by the University.

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.

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.

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 Head of Information Compliance & Policy.

**Students who process personal data**

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 data protection regulations and shall work under the direct supervision of a member of staff.

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**

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 website.
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.

In cases where sensitive personal data is being processed, researchers shall need to get the approval of the Ethics Committee before commencing processing. In cases where research data is to be shared with other researchers based overseas, the explicit consent of the research subjects shall be sought.

References

References issued on behalf of the University should largely comprise brief statements of fact and minimal opinion. Where opinion is given, it should be supported with factual evidence wherever possible. All staff shall be made aware that references they write may become available to the subject in certain circumstances.

In cases where references are written for internal consumption only (for example, by use in a promotions panel) these shall be made available to the subject on request unless this would lead to an unavoidable disclosure of some other third party’s personal details. If you are unsure you should seek advice from the Human Resources Department.

References received by the University should be made available to the subject on request. All standard reference request forms should make this clear to the referee, and all departments should ensure that referees are fully aware of the possibility of subject access.

Examination marks

Students shall be informed of marks for coursework at the time of their award. Examination marks usually shall be made available to students in the form of formal transcripts of marks, which shall be forwarded to students as soon as is practically possible. If so requested, marks must be released to debtors no more than 40 days after their official release (or 5 months from the date of request if this is sooner), though such release will not be by formal transcript.

Web

The University maintains a strong web presence. Basic personal details for all relevant staff will be provided on the web-site, though any member of staff may appeal to their Head of Department if they feel that the display of their details (or some part thereof) would cause them unwarranted damage or distress.

Students’ details (including email addresses) shall not be displayed on the University web-site, except with the explicit consent of the individuals involved (this includes images of students who appear on promotional photographs etc.).

Web cameras should not be used where these provide images of identifiable individuals.
CCTV

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.

All CCTV images have ownership and copyright vested in City University. Consent to use or reproduce material held by the University resulting from the CCTV system will normally be withheld. All cameras will be mounted in public view and signs will be displayed warning of their presence and the purposes of their operation.

Data on tapes will normally be preserved for one month. After this period, if they are not needed for evidential purposes, the tapes will be re-used. If required for evidential purposes, they will be retained for as long as is necessary to the prosecution of the case. Individuals may request in writing that they see a tape they believe may hold images of them. This request should be made through the standard Subject Access Request procedure (though in the latter case the subject will have to specify that they wish the standard search to cover CCTV images).

Implementation & Guidance

Further information on the Data Protection Act and how it applies to your area can be sought from the Head of Information Compliance and Policy.
# Appendix 1: Glossary of terms

<table>
<thead>
<tr>
<th><strong>Assessment</strong></th>
<th>Review of a data controller’s processing activities conducted by the Information Commissioner following a request by a data subject.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Data subject</strong></td>
<td>Anyone whose personal information is processed by a data controller.</td>
</tr>
<tr>
<td><strong>Direct marketing</strong></td>
<td>The sending of solicited or unsolicited mail (including email) designed to promote the activities of the data controller.</td>
</tr>
<tr>
<td><strong>Explicit consent</strong></td>
<td>Consent given positively by a data subject who has been clearly informed of a data controller’s reasons for processing data. Failure to respond to a mailing <em>cannot</em> be interpreted as explicit consent, though failure to complete an opt-out box on a form that has otherwise been completed by a subject <em>can</em> be interpreted as explicit consent.</td>
</tr>
<tr>
<td><strong>Notification</strong></td>
<td>Confirmation of all processing activities conducted by the data controller and lodged with the Office of the Information Commissioner as a matter of record.</td>
</tr>
<tr>
<td><strong>Relevant filing system</strong></td>
<td>Any filing system that is structured with reference to individuals (or criteria relating to individuals). All filing systems at the University, however haphazard, should be assumed to match this definition.</td>
</tr>
<tr>
<td><strong>Personal data</strong></td>
<td>Information (including photographic or other images) relating to identifiable <em>living</em> individuals.</td>
</tr>
<tr>
<td><strong>Processing</strong></td>
<td>Collection, storage, analysis, disclosure, destruction, or modification of personal data.</td>
</tr>
<tr>
<td><strong>Subject access request</strong></td>
<td>Request made by a data subject requiring a data controller to release to them (in hard copy form, unless otherwise stated by the subject) all data held about them.</td>
</tr>
<tr>
<td><strong>Vital interests</strong></td>
<td>Realistically, the life of the subject (or, at least, the continued well-being of the subject).</td>
</tr>
</tbody>
</table>
Appendix 2: The Eight Principles

Greater detail about these principles can be found in the Information Commissioners 'Data Protection Act 1998: Legal Guidance'

**Principle 1:** Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless at least one [appropriate] condition is met.

**Relevant conditions for processing data:**

- The data subject has given consent
- Processing is necessary for the performance of a contract to which the data subject is a party
- Processing is necessary for compliance with any legal obligation placed on the controller
- Processing is necessary to protect the vital interests of the data subject
- Processing is necessary for the purposes of legitimate interests pursued by the data controller or by third parties to whom the data is disclosed (except where this might prejudice the rights or freedoms of the data subject).

**Relevant conditions for processing sensitive data:**

- The data subject has given *explicit* consent
- Processing is necessary for compliance with any legal obligation placed on the controller that relates to employment
- Processing is necessary to protect the vital interests of the data subject
- The information involved has already been made public by the subject
- Processing is necessary for the purposes of / in connection with legal proceedings
- Processing is necessary for reviewing equality of opportunity (relates to ethnicity data only)

**Principle 2:** Personal data shall be obtained for one or more specified and lawful purposes and shall not be processed in any manner incompatible with those purposes.

**Principle 3:** Personal data shall be adequate, relevant and not excessive to the purposes for which they are processed.

**Principle 4:** Personal data shall be accurate and, where necessary, up to date.

**Principle 5:** Personal data processed for any purpose shall not be kept for longer than is necessary for that purpose.

**Principle 6:** Personal data shall be processed in accordance with the rights of data subjects under the Act.
**Principle 7:** Appropriate measures shall be taken against unauthorised processing of personal data and accidental loss or destruction of personal data

**Principle 8:** Personal data shall not be transferred to a country outside the EEA unless –

- The data subject has given consent
- Transfer is necessary for the performance of a contract to which the data subject is a party
- Transfer is made for reasons for substantial public interest
- Transfer is necessary to protect the vital interests of the data subject
- Transfer is necessary for the purposes of / in connection with legal proceedings
Appendix 3: Sensitive data

The Act defines sensitive data as data relating to:

- Ethnic origin
- Political opinion
- Religious beliefs
- Trade Union membership
- Physical and mental health
- Sexual life
- Criminal record

The University undertakes to process sensitive data only where the relevant conditions apply. Staff are advised not to collect sensitive data unless there is proven need for this information. The circumstances in which the University accepts that sensitive data will have to be processed are as follows:

- The provision of pastoral support to students.
- The compilation of relevant monitoring data for government agencies (e.g. HESA).
- Research.
- Staff and student review and appeal processes.
- Admissions processes (in relation to criminal record information).

If staff wish to process data for reasons other than those given above, they should contact the Head of Information Compliance & Policy for advice before commencing processing.
Appendix 4: Staff responsibilities

The Director for Information shall be responsible for

- Overall responsibility for Data Protection

The Head of Information Compliance & Policy shall be responsible for:

- Maintaining the University’s notification.
- Reviewing this policy annually.
- Reporting to the Senior Management Group on issues of importance relating to Data Protection.
- Providing advice to Heads of Departments and other managerial staff on Data Protection issues.
- Co-ordinating response to any Subject Access Request

The Director of Computing Services shall be responsible for:

- The security (including appropriate back-up procedures) of all personal data on University computer systems

Heads of Departments shall be responsible for:

- Ensuring that data processing operations in their departments comply with this policy.