Kingston University London

Code of Practice for the Consideration of Third Party Requests for Personal Data Citing Section 29(3) of the Data Protection Act 1998

1. Introduction

1.1 From time to time the University may receive requests from the police or other organisations (such as local authority or NHS fraud investigation units) for the disclosure of information relating to an identifiable individual that is required in connection with the prevention or detection of crime, the apprehension or prosecution of offenders, or the assessment or collection of tax. Whilst in many cases it is likely to be in the public interest to assist such bodies by providing the requisite information, the University is committed to ensuring that all such disclosures are fair and lawful, and in particular, that they are compliant with the Data Protection Act 1998 ('the Act'). This Code of Practice has been developed by the University Secretary's Department to provide the necessary framework for ensuring that all such requests are treated in a consistent, lawful, and appropriately documented fashion.

2. Data Protection Officer Contact Details

2.1 The contact details of the Data Protection Officer for Kingston University and its subsidiary companies, including Kingston University Service Company Ltd (KUSCO), are as follows:

- Address: University Secretary's Department, Kingston University, River House, 53-57 High Street, Kingston upon Thames, Surrey, KT1 1LQ;
- E-mail: s.weir@kingston.ac.uk;
- Telephone: 020 8417 3026 (Internal: 63026).

3. Statutory Basis for Disclosure

3.1 Personal data are defined in the Act as biographical data relating to a living individual who can be identified either from those data alone, or from the data in

conjunction with additional data held by, or likely to come into the possession of, the data controller. A data controller is the person (or organisation) who determines how personal data are to be processed. In the case of personal data held by the University, the institution is the data controller; following any disclosure, the recipient becomes the data controller in respect of the information concerned.

3.2 Schedule 1 of the Act requires data controllers to comply with eight Data Protection Principles. The first Principle states that 'Personal data shall be processed fairly and lawfully, and in particular, shall not be processed unless – (a) at least one of the conditions in Schedule 2 is met, and (b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.'

3.3 The Act stipulates that in order for processing to be fair, an individual who is the subject of any personal data to be processed (the 'data subject') must be provided with details of the purposes for which that processing will take place, together with any other information that is relevant in the specific circumstances.

3.4 However, section 29(3) of the Act provides an exemption from, inter alia, the requirement to provide fair processing information to the data subject where the processing is necessary for the purpose of the prevention or detection of crime, the apprehension or prosecution of offenders, or the assessment or collection of any tax or duty, to the extent that providing the fair processing information would prejudice the purpose.

3.5 Whilst section 29(3) provides an exemption from the first Principle to the extent outlined in paragraph 3.4 above, it is still necessary in respect of any prospective disclosure citing the exemption to satisfy at least one Schedule 2 condition, and in the case of sensitive personal data (relating to a data subject's race or ethnic origin, political opinions, religious (or similar) beliefs, health, sexual life, or the actual or alleged commission of an offence, together with any proceedings brought in relation to the latter) at least one Schedule 3 condition.

3.6 Schedule 2 conditions which are most likely to obtain in respect of a request for disclosure under section 29(3) of the Act are that:

(3) The processing is necessary for compliance with any legal obligation to which the data controller is subject, other than an obligation imposed by contract.

(5) The processing is necessary –

(a) for the administration of justice,

(b) for the exercise of any functions conferred on any person by or under any enactment,

(d) for the exercise of any other functions of a public nature exercised in the public interest by any person.

3.7 Schedule 3 conditions in the Act which are most likely to obtain in such circumstances are that:

(7(1)) The processing is necessary –

(a) for the administration of justice,

(b) or the exercise of any functions conferred on any person by or under an enactment

(7A(1))The processing –

(a) is … -

(i) the disclosure of sensitive personal data by a person as a member of an anti-fraud organisation or otherwise in accordance with any arrangements made by such an organisation;

(b) is necessary for the purposes of preventing fraud or a particular kind of fraud.

3.8 Additional circumstances in which processing of sensitive personal data is permitted by the Data Protection (Processing of Sensitive Personal Data Order) 2000, and which may obtain in respect of a section 29(3) request are when:

(1) (1) The processing –

(a) is in the substantial public interest;

(b) is necessary for the purposes of the prevention or detection of any unlawful act; and

(c) must necessarily be carried out without the explicit consent of the data subject being sought so as not to prejudice those purposes.

(2) In this paragraph, “act” includes a failure to act.

(10) The processing is necessary for the exercise of any functions conferred on a constable by any rule of law.

3.9 In the event that at least one Schedule 2 condition obtains, together with at least one Schedule 3 condition in respect of sensitive personal data, it is not necessary for the consent of the data subject to be secured prior to disclosure. However, the data subject should be informed that the disclosure is going to be

made unless doing do will prejudice the purposes for which the data are to be provided.

3.10 It should be noted that whilst the section 29(3) exemption permits the disclosure of personal data where necessary in connection with one of the specified purposes, it is entirely at the University's discretion whether it provides a substantive response unless it is required to do so by law, i.e. where it is under a statutory obligation to disclose or it is served with a court order compelling it to do so. Under such circumstances section 35(1), Schedule 2, Condition 3, and Schedule 3, Condition 7(1)(a) will be engaged.

3.11 The seventh Data Protection Principle requires appropriate technical and organisational measures to be taken against unauthorised or unlawful disclosure of personal data. Accordingly the University must be satisfied as to the veracity of any request citing the section 29(3) exemption, and must ensure that any method by which data are disclosed is appropriately secure given the nature of the data concerned in any particular circumstance.

4. Responsibilities

4.1 The Data Protection Officer, based in the University Secretary's Department, maintains oversight of the process for responding to requests for information from third parties citing the section 29(3) exemption, and documents the receipt, processing, and disclosure of data in response to, such requests.

4.2 As a general principle, the Data Protection Officer will assess relevant requests, collate data as appropriate, and provide responses. However, it is acknowledged that in some circumstances it is appropriate for specified members of staff to collate data and provide responses, with appropriate authorisation from the Data Protection Officer, by virtue of their responsibility for the data requested, or in view of relationships maintained with requesting organisations.

4.3 Accordingly, the following members of staff are authorised to compile and return responses to section 29(3) requests, following consultation with the Data Protection Officer, in respect of the data types specified below.

Member of Staff	**Department**	**Personal Data Types**
Head of Accommodation Services	Accommodation Services	Tenancy Data
Head of Support Services/Security	KUSCO	CCTV Footage

Manager		
Access Control System Manager	KUSCO	Access Control Records

4.4 Members of staff working in the above departments who receive a request citing section 29(3) for data of the relevant type should forward the request to the specified individual for action.

4.5 All other requests for disclosure of personal data received by staff that cite the section 29(3) exemption, or any request citing any other exemption in the Act, should be forwarded to the Data Protection Officer as promptly as possible.

5. The Process

5.1 Upon receipt of a section 29(3) request made by e-mail or telephone, as a measure of security the Data Protection Officer (or other authorised member of staff, as per paragraph 4.3 above) will ask that the request is resubmitted in a letter. The letter should:

(a) Be on the requesting organisation's headed paper;

(b) State the section of the Act under which the request is being made (together with any other statutory basis for disclosure that is considered to apply, if appropriate);

(c) Specify in as much detail as possible the data that are sought;

(d) State, in as much detail as possible in the circumstances, the purpose(s) for which the data are requested;

(e) State, if this is the case, that a failure to disclose would prejudice the purpose(s) for which the data are requested;

(f) Be signed by the requestor and countersigned by their supervisor, and provide the name, position and full contact details of both including address, telephone number and e-mail address.

5.2 Where requests are made by the police, rather than providing a letter the force's Personal Data Request Form, based on the template in Appendix F of the Association of Chief Police Officers' Data Protection Manual of Guidance, should be provided. In the case of the Metropolitan Police this is Form 3022. The form must be completed in accordance with its own requirements and as fully as necessary in the circumstances.

5.3 Upon receipt of a written request satisfying the requirements of 5.1 or 5.2 above, the Data Protection Officer (or other authorised member of staff) will obtain the requested data from University databases (e.g. the SITS student records system), and/or from faculty/department staff as appropriate. In the case of the latter, requests for data will be made to the nominated faculty/department data protection contact.

5.4 In the case of requests received and processed by the Data Protection Officer, following collation of the requested data he/she will make a judgment whether:

- A Schedule 2 condition (and in the case of sensitive personal data, a Schedule 3 condition) obtains;
- Disclosure of any or all of the requested data is necessary for the purposes for which they are requested, i.e. whether a failure to disclose the data would prejudice the stated purposes;
- Notification of the data subject of any intended disclosure would prejudice the stated purposes.

5.5 The Data Protection Officer will complete the Data Sharing Decision Form at Annex A, and will contact the requestor in writing using the response template at Annex B, supplying data to the extent that the above criteria are satisfied.

5.6 In the case of requests received and processed by authorised members of staff, following collation of the requested data, the member of staff will draft a response to the requestor using the response template at Annex B and will forward this to the Data Protection Officer with copies of the original request and the requested data.

5.7 Where the request is for a copy of CCTV footage, the footage itself need not be provided to the Data Protection Officer by the authorised member of staff, but a description of the images depicted should be forwarded with the other documentation. A copy of the footage should however be retained by the authorised member of staff.

5.8 The Data Protection Officer will determine whether the criteria in paragraph 5.4 above are satisfied, and will advise the authorised member of staff of any alterations required to the draft response in view of his/her decision. The authorised member of staff will subsequently respond to the request accordingly in writing, copied to the Data Protection Officer; the latter will complete the Data Sharing Decision Form at Annex A.

5.9 For every section 29(3) request received, the following documentation will be retained on file in an Exceptional Disclosures Log by the Data Protection Officer:

(1) The completed Data Sharing Decision Form;

(2) The original request and any subsequent correspondence;

(3) Copies of all data requested;

(4) Any draft response and amendments requested by the Data Protection Officer, where relevant.

(5) A copy of the final response to the request, including any data disclosed.

6. Format of Correspondence

6.1 The default method of disclosing any personal data in response to a section 29 request will be in writing by post to the address provided in the written request. Wherever possible steps will be taken to verify the authenticity of the address provided, e.g. by undertaking an internet search for the requesting organisation. Depending on the nature of the data being disclosed, the use of recorded delivery may be appropriate.

6.2 However, notwithstanding the above, it is recognised that on occasion the nature of an investigation may be such that it is appropriate both to receive the request, and to provide a response, by e-mail, whilst recognising that e-mail is not a secure method of communication. In such circumstances, the request and response must still be provided in the format prescribed above, including signatures, but can be attached to the e-mail as a scanned file. The destination e-mail address must match that provided in the request and must be readily verifiable as belonging to the requesting organisation. Where the nature of the data is such that the risk of providing them by e-mail is deemed too great, the possibility of supplying them by facsimile transmission should be explored.

6.3 The disclosure of personal data by telephone in response to a section 29(3) request will only be made in exceptional circumstances by, or on the direct authorisation of, the University Secretary, or by the duty member of the Executive Board outside core hours.

6.4 In some circumstances, e.g. in respect of CCTV footage, data may be collected in person by the requesting individual. Disclosure in person is only permitted where: the process outlined above in section 5 has been followed; the appointment for collection has been pre-arranged with the authorised member of staff; upon arrival a photocopy of the requesting individual's warrant card/organisation photographic identity card is taken; and the requesting individual signs and dates a copy of the completed response template. Copies of the card and

the signed response template should be forwarded to the Data Protection Officer following the disclosure for retention in the Exceptional Disclosure Log.

7. Status of CCTV Footage

7.1 In accordance with section 3 of the Information Commissioner's CCTV Code of Practice, the University considers footage of potentially identifiable individuals to be subject to the Act. Accordingly, any request for disclosure of CCTV footage with a view to identifying individuals depicted must be made in accordance with the requirements of this Code of Practice, even where that request is not made with reference to named individuals and/or where the University is not itself able to identify individuals from the footage concerned.

8. References

8.1 The following documents have been consulted in preparing this Code of Practice:

- Data Protection Act 1998
  http://www.legislation.gov.uk/ukpga/1998/29/contents
- The Data Protection (Processing of Sensitive Personal Data) Order 2000
  http://www.legislation.gov.uk/uksi/2000/417/contents/made
- Information Commissioner's Data Sharing Code of Practice
  http://www.ico.gov.uk/for_organisations/data_protection/topic_guides/~/media/documents/library/Data_Protection/Detailed_specialist_guides/data_sharing_code_of_practice.ashx
- Information Commissioner's CCTV Code of Practice
  http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/ico_cctvfinal_2301.pdf
- ACPO Data Protection Manual of Guidance – Part I: Standards
  http://www.acpo.police.uk/documents/information/2010/201002INFDPMOG01.pdf

University Secretary's Department

August 2011

Annex A

Data Sharing Decision Form

Name of requesting organisation	
Name and position of requesting individual	
Date request received	
Request received and processed by	
Personal data requested	
Specified purpose	
Schedule 2 condition(s) obtaining (if appropriate)	
Schedule 3 condition(s) obtaining (if appropriate)	
Data disclosed / withheld	
Decision taken by	
Date of disclosure	
Signed	
Dated	

To be attached:

- Original request and any subsequent correspondence;
- Copies of all data requested;
- Any draft response and revisions requested by the Data Protection Officer where relevant;
- A copy of the final response to the request, including any data disclosed.

Annex B

Response Template

Dear [name]

Re: Request for Disclosure of Personal Data – [Name of Data Subject]

Thank you for your letter/form *[delete as applicable]* dated [date] in which you request personal data relating to the above-named individual pursuant to section 29(3) of the Data Protection 1998. In response to your request I can advise that the following data are held on record by the University.

[Data, or description of data enclosed separately]

Please note that these data are provided solely for the purpose of [purpose] as set out in your letter/form *[delete as applicable].*

Yours sincerely,

[Name]

[Position]

[Department]

cc. Kingston University Data Protection Officer