



GLASGOW
CALEDONIAN
UNIVERSITY

Data Protection Guidelines (Version 2)

November 2005

Preface

These Guidelines are intended to promote good practice and assist members of the University in processing personal information in accordance with the Data Protection Act (1998). They are not intended to be an overview or summary of the Act but have been drafted in accordance with the Data Protection legislation and the Codes of Practice issued by the Information Commissioner.

As a responsible user of personal information the University supports the eight principles laid down in the Data Protection Act (1998). Infringements of this Act are *criminal offences* which carry legal penalties.

This Act has serious implications for ALL members of the University (staff and students). It covers both electronic and paper based *personal information, transfer of data abroad, direct marketing and security*. It determines the way personal information is collected, used and disclosed.

The Act is not about preventing the collection and use of personal information but ensuring that it is done in a way that respects the privacy of the individual in accordance with current legislation. ***Members of the University may use personal information for management, administration, research, etc. as required to undertake their job or studies but must ensure that they conform to these Guidelines.***

The University is required to notify the Information Commissioner, every September, as to the personal data it holds, what it is being used for and to whom it may be disclosed. The University's Notification, together with other useful information, can be found on the Information Commissioner's web site at www.informationcommissioner.gov.uk .

Additionally, a University Data Protection web site (www.gcal.ac.uk/datap/) has been set up to provide

- a quick/interactive search of the University's Data Protection Guidelines
- information on Subject Access Requests, including forms
- various guidelines (e.g. writing references, dealing with enquiries, retention periods, taking photographs, etc.)
- frequently asked questions
- sources of additional information

Pat McKay
Head of Information Strategy Unit
Designated Data Controller

Contents

1.	Introduction	4
2.	Definition: Data Subject	4
3.	Definition: Personal data	4
4.	Definition: Sensitive personal data	5
5.	Definition: Processing	5
6.	Definition: Automated decision making	5
7.	Data collection	5
8.	Data collection: Data to be collected	6
9.	Data collection: Photographs and videos	6
10.	Data collection: Data Subjects rights	6
11.	Data collection: Notification	7
12.	Accuracy	7
13.	Security	8
14.	Destruction of personal data	8
15.	Disclosure of personal data	8
16.	Rights of the Data Subject/Individual	9
17.	Transmission of personal data abroad	9
18.	Research, history and statistics	10
19.	Examination scripts and marks	10
20.	Coursework containing personal information	10
21.	Confidential references	10
22.	Direct marketing	11
23.	Staff responsibilities with respect to DPA	11
24.	Student responsibilities with respect to DPA	12
Appendix A	European Economic Area (EEA) Countries and other countries with adequate level of protection	13
Appendix B	Sample Form for Fair Collection of Personal Data	14
Appendix C	Suggested Retention Period	15
Appendix D	Photography and the Data Protection Act (1998)	17
Appendix E	Typical documentation for Requests for personal information from the Police	20
Appendix F	Guidelines for Writing References for Students	21
Appendix G	Standard Request Form for Access to Personal Data (Student)	23
Appendix H	Standard Request Form for Access to Personal Data (Staff)	24

1. Introduction

- 1.1 This document sets out Guidelines for members of the University, or others, who process or use any personal information on behalf of the University to ensure that the Data Protection Principles are met.
- 1.2 The University needs to keep certain information about its employees, students and other users. For example to allow it to monitor performance and achievements, ensure health and safety, pay staff, recruitment, programmes organised and legal obligations to funding bodies and government.
- 1.3 The Data Protection Act 1998 (the Act) is not about preventing the collection and use of personal information but ensuring that it is done in a way that respects the privacy of the individual.
- 1.4 Members of the University may use personal information for management, administration, research, etc. as required, to undertake their job but must ensure that they conform to these Guidelines. The information *belongs to the University*.
- 1.5 Members of the University, or others, may *not* use or process personal information, held by the University, for their own personal use.
- 1.6 To comply with the Act, information must be collected and used fairly, stored securely and not disclosed to any other person unlawfully. To do this, the University must comply with the Data Protection Principles which are set out in the Act. In summary these state that personal data shall:
 - (i) Be obtained and processed fairly and lawfully and shall not be processed unless certain conditions are met.
 - (ii) Be obtained for a specified and lawful purpose and shall not be processed in any manner incompatible with that purpose.
 - (iii) Be adequate, relevant and not excessive for those purposes.
 - (iv) Be accurate and kept up to date.
 - (v) Not be kept for longer than is necessary for that purpose.
 - (vi) Be processed in accordance with the data subject's rights.
 - (vii) Be kept safe from unauthorised access, accidental loss or destruction.
 - (viii) Not be transferred to a country outside the European Economic Area, unless that country has equivalent levels of protection for personal data [Appendix A].
- 1.7 A University Data Protection web site (www.gcal.ac.uk/datap/)has been set up to provide
 - a quick/interactive search of the University's Data Protection Guidelines
 - information on Subject Access Requests, including forms
 - various guidelines (e.g. writing references, dealing with enquiries, etc.)
 - frequently asked questions
 - sources of additional information

2. Definition: Data Subject

- 2.1 The *Data Subject* is the individual on whom data is being kept - e.g. a student, member of staff, applicant, customer, supplier, etc.

3. Definition: Personal data

- 3.1 It is *personal data* if
 - it relates to a living individual
 - it affects the person's privacy (personal, family life, business or professional)
 - the information is biographical in a significant sense (i.e. it must go beyond noting the individuals attendance at a meeting or involvement in matter which is not about him personally)
 - the information has the individual as its focus.

- 3.2 Personal data covers both *facts* and *expressed opinions* about the individual.
- 3.3 Personal data can be text and/or images (pictures and photos).
- 3.4 Personal data can be held on a computer (e.g. databases, word processed documents, email, Internet), on paper or on CCTV.
- 3.5 Examples of *personal data/information* are
- A named individual's salary
 - A named student's assessment marks
 - A reference for a student or member of staff
 - Personal information (e.g. home address, home telephone number, personal email address, date of birth, qualifications, etc.) of a named individual.
 - Lists of student names with placement details
- 3.6 Examples which are not *personal data/information*
- Attendance at meetings or mention in minutes, unless the meeting is about the named individual (e.g. names of individuals attending an assessment board are not personal information, but discussion about a particular student is)
 - University email addresses and telephone numbers
 - Names on sent or copied to parts of emails, memos, letters, etc. unless the body of the document is about the named individual

4. Definition: Sensitive personal data

- 4.1 *Sensitive personal data* includes racial or ethnic origin, political opinions, religious beliefs, trade union membership, physical or mental health, sexual life, commission or alleged commission of an offence and any proceedings from it.
- 4.2 Sometimes it is necessary to process [see §5] information about a person's health, criminal convictions, race and gender. This may be to ensure the University is a safe place for everyone, or to operate other University policies, such as the sick pay policy or equal opportunities policy, etc.
- 4.3 Processing of sensitive personal information may cause particular concern or distress to individuals, hence, normally, they must be asked for their *express consent* before the University can process it [see §10].
- 4.4 Sensitive data can be processed if it is to protect the vital interests of the individual or another person subject to the following conditions. The individual cannot give consent themselves (e.g. is physically incapable of doing so at the time) or where the University cannot be expected to obtain consent because the individual cannot be located. An example of processing/disclosing sensitive information under these conditions would be medical health emergency situations [see §10].

5. Definition: Processing

- 5.1 *Processing* includes obtaining/collecting, recording, holding, storing, organising, adapting, altering, aligning, combining, blocking, erasing and destroying the information or data.
- 5.2 It also includes carrying out any operation or set of operations on the information or data, including retrieval, consultation, use and disclosure.

6. Definition: Automated decision making

- 6.1 *Automated decision making* occurs when a decision is made by a computer without human intervention - e.g. calculation of assessment marks by computer which are not considered or ratified by a member of staff.
- 6.2 If *automated decision making* is being used then the students must be informed of this.

7. Data collection

- 7.1 Before collecting and recording personal data you should consider the following checklist
- (i) Do you really need to record the information?
 - (ii) Is the information 'sensitive'? If so, does it conform with the requirements in §4.
 - (iii) Has the data subject been told that this type of data will be processed?
 - (iv) Are you authorised to collect/store/process the data?
 - (v) Have you checked with the data subject that the data is accurate?
 - (vi) Are you sure that the data will be secure?
 - (vii) How long will the data be kept for? [See Appendix C].
 - (viii) If you do not have the individual's consent to process, are you satisfied that you are conforming to these Guidelines and all appropriate legislation?
 - (ix) Have you informed your School/Department Data Protection Rep that you will be collecting this personal data to ensure that it is covered by the University's Data Protection Notification [see §11.2]?
- 7.2 When collecting personal information you must inform the data subject
- who the Data Controller is (i.e. Glasgow Caledonian University),
 - its Designated Data Controller (i.e. Head of Information Strategy Unit)
 - what information the University holds and processes about them
 - why it processes the information
 - how long the information will be kept
 - to whom this will be disclosed
 - how they can gain access to it
 - how it is kept up to date
 - whether they will be the subject of any automated decision making
 - and that “*The University processes information in accordance with the Data Protection Act 1998*”
- A typical form that may be used for this purpose can be found in Appendix B.

8. Data collection: Data to be collected

- 8.1 Any personal data must be *obtained and processed for specified purposes*. It is illegal to use personal data that was collected for one purpose for another – e.g. the University collects personal data about students via their Registration Form for appropriate University business and to satisfy legal requirements, it therefore cannot be used for projects and/or research.
- 8.2 The personal data that is collected must be *adequate, relevant and not excessive*. There must be a specific reason why we need a specific piece of data. It is unlawful to collect data just in case it may be useful later on.
- 8.3 It is essential that the length of time that the personal data needs to be kept is determined before collecting it. Personal data must *not be held longer than necessary*. [See Appendix C for suggested retention periods]

9. Data collection: Photographs and videos

- 9.1 Photographs or videos in which individuals can be identified are personal data and therefore covered by the Act.
- 9.2 Refer to Appendix D for guidelines that need to be followed when taking photographs or making videos.

10. Data collection: Data Subjects rights

- 10.1 In some cases, the University can only process personal data with the consent of the individual - e.g. publishing personal information on the University web site would mean that it is being disclosed outside the EEA [see §1.6 (viii)].
- 10.2 If the data is sensitive, *express consent* should normally be obtained. However there are some circumstances where this is not the case [see §4].

- 10.3 Agreement to the University processing some specified classes of personal data is a condition of acceptance of a student onto any programme or a condition of employment for staff. This includes information about previous criminal convictions. Some jobs or programmes will bring the applicants into contact with children. The University has a duty under the Children Act and other enactments to ensure that staff are suitable for the job, and students for the programmes offered. The University also has a duty of care and must make sure that staff and students who use the University facilities do not pose a threat or danger to other users.
- 10.4 All prospective staff and students will be asked to sign an appropriate form (i.e. employment contract or online Registration Form), indicating what personal data is being collected, what it will be used for and to whom it may be disclosed when an offer of employment or a place on a programme is made. A refusal to sign such a form can result in the offer being withdrawn.
- 10.5 The University also asks for information about particular health needs, such as allergies to particular forms of medication, or any conditions such as asthma or diabetes. This information may only be used in the protection of the health and safety of the individual (i.e. their vital interests), and can be processed without their consent if they are unable to provide it [see §4.4] for example in a medical emergency.
- 10.6 When collecting *any* personal data the Data Subject *must* be given the information in §7.2

11. Data collection: Notification

- 11.1 All personal data and information held by the University, either centrally or by departments, *must* be notified annually to the Information Commissioner. This is undertaken through the Information Strategy Unit (ISU).
- 11.2 Annually in August ISU asks Schools/Departments to complete a Data Protection Audit. This requires them to specify any additional personal information or uses of existing information during the previous year. For such personal information the following must be provided:
- a description of the personal data being held
 - a description of the purpose for which the data is being processed
 - a description of the intended disclosure of the information
 - countries outside the EEA [see Appendix A] to which personal data may be transferred
 - a description of the general security measures that are used to protect this data
- 11.3 It is important that the Data Protection Audit is completed satisfactorily as there is a legal obligation on the University to ensure that the Information Commissioner is notified of all the processing of personal information that is being undertaken. Failure to do so is an offence which can result in a fine (and unwanted publicity!!!).

12. Accuracy

- 12.1 Personal data and information *must be kept accurate and up to date*. This includes both central administrative systems and department based systems whether held on computer or paper.
- 12.2 Holding duplicate information leads to inaccuracies and extra care must be taken to ensure that *all* copies of personal data are updated. Holding duplicate information by departments (on computer or record cards) can lead to infringements of the Act – e.g.(1) Department X updated their records when informed by students of changes to address and/or telephone number but failed to inform the Academic Registry leading to the Central Student Record System (CSRS) being inaccurate; e.g.(2) Department Y downloaded student information from the CSRS but failed to do this regularly and hence sent information to addresses that were more than a year out of date although the students had kept CSRS informed of any changes. *Both these examples are an*

infringement of the Act and the Data Subject has the right to complain to the Information Commissioner.

- 12.3 The *primary source of student personal data is CSRS (OMNIS)* and departments must ensure that it is kept accurate and up to date.
- 12.4 The *primary source of staff personal data is the HR department* and members of staff must ensure that they are kept informed of any changes/updates.

13. Security

- 13.1 All personal data *must be kept secure* from unauthorized access.
- 13.2 For computer based information this would include the use of passwords, password protected screensavers, ensuring that personal information is not left displayed on a screen, disks/CDs locked away, etc.
- 13.3 Particular care must be taken when holding personal information on laptop computers. Laptops should be locked away when not in use. Personal information held on laptops should be deleted as soon as it is no longer required..
- 13.4 Personal data/information held on paper should be kept in locked cupboards and/or drawers unless it is being worked on.
- 13.5 Refer to the University’s Communications & Information Technology and Systems Security Policy can be found at http://www.learningservices.gcal.ac.uk/it/policies/security_policy.html
- 13.6 Further information on acceptable security standards can be found in BS7799 available from the British Standards Institute. A copy is held in the University Library.

14. Destruction of personal data

- 14.1 When obtaining personal data the length of time it needs to be kept should already have been determined [see §8.3].
- 14.2 Personal data must be treated as confidential information and destroyed appropriately.
- 14.3 If held on a computer it must be deleted from *all* files and archives. To ensure that personal information is completely erased from computers contact IT Helpdesk for assistance (note that deleting a file does not erase the data from the hard disk).
- 14.4 If held in another form it should be shredded.

15. Disclosure of personal data

- 15.1 The collection [see §8] and notification [see §11] of personal data indicates what disclosures can *legally* be made and to whom.
- 15.2 Information about staff or students *cannot* be disclosed without their consent. This includes confirming that they are students or members of staff of the university. Disclosing information to fellow students, family, employers etc. needs careful consideration - e.g. “My pal is not in today and I need to contact her about a group project. Can I have her phone number?” Even if you know they are friends and working on the same group project it is illegal to give out the phone number or any other personal details.
- 15.3 Displaying personal information (e.g. staff, student photographs and bibliographies) on the Internet or Notice Boards requires the explicit consent of the individual. In giving their consent members of the University must be made fully aware that this information will be then be available to countries where their personal information will not be protected.
- 15.4 Any external requests for information about staff or students must be put in *writing* on appropriate headed notepaper containing telephone and/or fax numbers that could be checked out. Asking for the request to be put in writing will not be an issue if it is bona fide and will provide some protection from ‘bogus’ enquirers – e.g. a telephone request

from an individual claiming to be from a Home Office department wanting information about a student which he was not prepared to put in writing – on checking with the Home Office neither the Department nor the individual existed.

- 15.5 Requests other than from the individual themselves should be treated as Freedom of Information requests. If it is the type of request that you would normally respond to as part of normal business (e.g. a reference) then handle it as normal otherwise pass the request to your FoI Forum Representative.
- 15.6 The Police *do not* have a right to personal information, however in certain circumstances we can disclose information to the Police. Requests from the Police should be in writing and on a form similar to that in Appendix E. All requests from the Police must be referred to the Information Strategy Unit.
- 15.7 Requests for *references* must be in writing. If a request for a reference for a job or further study is addressed to a *named* member of staff you can assume that the individual has given consent. In all other cases the request for a reference should be sent to the Department of Academic Administration who will respond to the enquiry by initially requesting confirmation that the individual knows this reference is being sought. (Information to assist writing references can be found in Appendix F).
- 15.8 Personal information can be disclosed to meet the University's legal requirements – e.g. Students Loan Agency, HESA, Inland Revenue, etc. Again, unless it is someone from these Agencies that you have regular dealings with ask for the request in writing. Most requests within this area are likely to be addressed to either the Department of Academic Administration or HR Department.
- 15.9 If staff or students are undertaking a *period of study and/or placement abroad* in countries out with the EEA [see §17 and Appendix A] then only personal information required to allow this to go ahead should be disclosed. In these circumstances express consent in the form of a signed agreement [e.g. Appendix C] must be given by the individual(s) concerned.

16. Rights of the Data Subject/Individual

- 16.1 Staff, students, etc. have rights with respect to any personal data that the University holds about them whether it is held on computer or in paper files. They can
 - *request* a copy of data/information held (*Subject Access Requests*)
 - have it *corrected*
 - *prevent* certain types of processing (e.g. automated decision taking, direct marketing, processing likely to cause substantial damage or substantial stress)
- 16.2 Subject Access Requests must be made in *writing* and provide sufficient information to allow the data to be readily retrieved. [Subject Access Forms in Appendices G(Student) and H(Staff) can be used].
- 16.3 *Subject Access Requests must be sent to the Information Strategy Unit accompanied by an administration fee of £10 (cheque made payable to Glasgow Caledonian University).*
- 16.4 The person making the request must provide sufficient evidence to allow the University to verify their identity (e.g. photographic evidence – staff card, matric card)
- 16.4 The requested information must be given to the requester within 40 days.

17. Transmission of personal data abroad

- 17.1 Personal data can be transferred to any country in the *European Economic Area* or a country that has similar data protection legislation [see Appendix A]
- 17.2 Personal data can only be transferred elsewhere, with the **consent** of the Data Subject this should include a caveat that *the University cannot guarantee the security of the information being transferred*. A caveat should be included with the transmission

indicating to the receiver of the information *that it may only be used for the purposes it was provided.*

- 17.3 Personal information put on the Internet or in external publications should be considered as being disclosed worldwide. Therefore the consent of the individual concerned must be obtained first. [Sample form see Appendix B]

18. Research, history and statistics

- 18.1 Where personal data is used for the purposes of research, history and statistics it
- must have been obtained fairly and lawfully [see §7]
 - is exempt from subject access as long it is not used to support measures or decisions with respect to a specific individual
 - must not be processed in a way that is likely to cause substantial damage or substantial stress to the Data Subject/individual
- 18.2 Where the data contains personal identifiers these must be irreversibly anonymised before disclosing to the researcher unless the researcher already knows the details and these details are necessary in order to carry out the research.
- 18.3 If the research uses personal information from an external organisation (e.g. part time students undertaking a project using their employer's personnel information) then you must ensure that the employer's Data Protection Notification includes an entry indicating that it uses employee information for research purposes. All Notifications can be viewed at <http://www.esd.informationcommissioner.gov.uk/esd/search.asp>
- 18.4 While research data can be held indefinitely good practice would dictate assessment and justification.
- 18.5 Personal data collected for a specific piece of research cannot be used for other/additional research without the consent of the data subject [see §7]. This can be obtained at the time as obtaining consent for the original research.

19. Examination scripts and marks

- 19.1 Examination scripts *belong* to the University and are exempt from disclosure; however students are *entitled* to any marks or comments written on the script.
- 19.2 Students are entitled to their marks for both coursework and examinations. *Unpublished* marks must be disclosed within 5 months of a Subject Access Request.
- 19.3 If there are outstanding fees, accommodation charges or books and equipment still to be returned then the University may withhold certificates, transcripts, accreditation or references *but cannot withhold marks.*

20. Coursework containing personal information

- 20.1 Where possible personal information used by students in coursework should be anonymous.
- 20.2 Where this is impossible it must be collected in accordance with these University Data Protection Guidelines.
- 20.3 Such coursework should not be kept longer than necessary and should then be shredded.

21. Confidential references

- 21.1 If a student or member of staff asks you to provide them with a reference you cannot include any information on health/medical issues (sensitive information) unless you have their *explicit* consent to do so.
- 21.2 Confidential references given by members of the University for specific purposes (e.g. employment, training) are exempt from access by the data subject.
- 21.3 References can be disclosed to the data subject by the recipient of the reference.

- 21.4 A data subject can ask, through a Subject Access Request (SAR), to see a reference that the University has received.
- 21.5 References written for internal purposes will be disclosed in response to a SAR.
- 21.6 When *asking* for references you should indicate that the University will disclose it in response to a SAR

22. Direct marketing

- 22.1 Direct marketing relates to communication (regardless of media) with respect to advertising or marketing material that is directed to individuals e.g. mail shots for fund raising, advertising short courses, etc.
- 22.2 For every direct marketing activity the individual must be given the opportunity to be removed from your databases/lists
- 22.3 *Initial contact* with an individual/data subject must *not* be done via email unless you already have a *warm* relationship with them – e.g. we have a *warm* relationship with our students, but not with Mr X from Company Y that we have found from a directory, an advertisement or bought something from.
- 22.4 Direct Marketing must also meet the regulations of the Telecommunications (Data Protection and Privacy) (Direct Marketing) Regulations 1998.

23. Staff responsibilities with respect to DPA

- 23.1 Members of staff are required to follow these Data Protection Guidelines when processing any personal information.
- 23.2 The University will implement these Data Protection Guidelines by ensuring that there is a general awareness of Data Protection issues through
 - publicising these Guidelines to all members of the University
 - a Data Protection web site
 - an online module on Blackboard
 - including Data Protection in Staff Induction Programmes
- 23.3 Deans/Heads are responsible for ensuring that members of their School/Department process information in accordance with these Guidelines.
- 23.4 Annually in August Schools/Departments are required to make a Data Protection Audit return to the Information Strategy Unit. This requires them to specify any additional personal information or uses of existing information during the previous year [see §11.2].
- 23.5 Every School/Department will have a Data Protection Officer nominated by the Dean/Head who will be able to provide relevant advice on data protection. They will be responsible to the Head of Department and liaise with the Information Strategy Unit.
- 23.6 A seminar for department Data Protection Officers to be held at least once per year.
- 23.7 Members of staff must include appropriate Data Protection statements on all documents that are used to collect personal information e.g. Student Registration Forms, Staff Contracts, etc. These statements must include informing the data subject of information being collected, its purpose and to whom it may be disclosed [see §7.2, Appendix 12]
- 23.8 Members of staff supervising student work must ensure that the students adhere to these Guidelines when using personal information.
- 23.9 Members of staff should provide advice as to how individuals can obtain copies of personal information held about them [see §15 and §16].
- 23.10 Members of staff receiving Subject Access Requests should pass them promptly to the Head of Information Strategy Unit

24. Student responsibilities with respect to DPA

- 24.1 Students are required to follow these Data Protection University Guidelines when processing any personal information as part of their studies/research.
- 24.2 The University will implement these Data Protection Guidelines by ensuring that there is a general awareness of Data Protection issues through
 - publicising these Guidelines to all members of the University
 - a Data Protection web site
 - an online module on Blackboard
- 24.3 Students are responsible for ensuring that they conform to these Guidelines when using personal information in undertaking their studies in and on behalf of the University.
- 24.4 Students must include appropriate Data Protection statements on all documents that are used to collect personal information e.g. Survey questionnaires. These statements must include informing the individual of information being collected, its purpose and to whom it may be disclosed [see §7.2].
- 24.5 Students who have any queries with respect to Data Protection or these Guidelines should seek advice from their tutor.

Appendix A European Economic Area (EEA) Countries and other countries with adequate level of protection

1. European Economic Area (EEA)

- Austria
 - Belgium
 - Cyprus
 - Czech Republic
 - Denmark
 - Estonia
 - Finland
 - France
 - Germany
 - Greece
 - Hungary
 - Ireland
 - Italy
 - Latvia
 - Lithuania
 - Luxembourg
 - Malta
 - The Netherlands
 - Poland
 - Portugal
 - Slovakia
 - Slovenia
 - Spain
 - Sweden
 - United Kingdom
 - Iceland¹
 - Liechtenstein¹
 - Norway¹
- ¹These countries are not members of the European Union (EU) but are included within the EEA.

2. Third countries with adequate level of protection

For up to date details refer the European Commissions web site at www.europa.eu.int/comm/justice_home/fsj/privacy/thridcountries/index_en.htm

To date (May 2005) the Europe Commission has recognized that the following countries have an appropriate level of data protection and hence personal data can be transferred without breaching Principal 8 (transfer of data out with the EEA):

- Argentina
- Canada
- Guernsey
- Isle of Man
- Switzerland

There is no general cover for the transfer of personal information to the U.S.A. However personal information can be transferred to U.S. organisations if they have signed up to the US Department of Commerce's Safe Harbor Privacy Principles.

Appendix B Sample Form for Fair Collection of Personal Data

The Data Protection Act 1998 seeks to ensure that your personal details are used fairly and lawfully and are kept secure. Under this Act the University is the Data Controller and must comply with certain obligations. One of these is to advise you of certain information including the purposes for which your information is being used.



GLASGOW
CALEDONIAN
UNIVERSITY

Department/Division: _____

I consent to the following personal information

being used for the purposes of

and that it could be disclosed to

The Data Protection Act gives you right of access to the personal data the University holds about you. You can exercise this right by making a request in writing to the *Information Strategy Unit, Glasgow Caledonian University, Cowcaddens Road, Glasgow G4 0BA* or email foi@gcal.ac.uk. The University requires payment of the £10 statutory fee before responding to the request.

The University collects, processes, secures and discloses personal information in accordance with the Data Protection Act 1998. Further information can be found at <http://home.gcal.ac.uk/datap/index.html>

Signed _____ Date _____

Name [Block letters] _____

Appendix C Suggested Retention Period

<i>Type Personal Information</i>	<i>Suggested Retention Period</i>	<i>Reasons</i>
Personnel files including training records and notes of disciplinary and grievance hearings.	6 years from the end of employment.	References and potential litigation.
Notes of disciplinary and grievance hearings if not kept in the personnel file	6 years from the settlement of the case	Limitation Act 1980
Application forms/interview notes	6 months from the date of the interview.	Time limits on litigation.
Income Tax and NI returns, including correspondence with tax office.	3 years after the end of the financial year to which the records relate.	Income Tax (Employment) Regulations 1993.
Statutory Maternity Pay records and calculations.	3 years after the end of the financial year to which the records relate.	Statutory Maternity Pay (General) Regulations 1986.
Statutory Sick Pay records and calculations.	3 years after the end of the financial year to which the records relate.	Statutory Sick Pay (General) Regulations 1982
Wage and salary records	6 years	Taxes Management Act 1970.
Facts relating to redundancies: Less than 20	3 years from date of redundancy	Time limits on litigation
20 or more	12 years from date of redundancy	Limitation Act 1980
Health records	During employment	Management of Health and Safety at Work Regulations.
Health records where reason for termination of employment is connected with health, including stress related illness.	3 years	Limitation period for personal injury claims.
Medical records kept by reason of the Control of Substances hazardous to Health Regulations 1994.	40 years	COSHHR 1994
Student records, including academic achievements and conduct	6 years from the date the student leaves the University, in case of litigation for negligence. 10 years for personal and academic references, with the agreement of the student.	Limitation period for negligence.
Application forms for unsuccessful candidates	6 months from start of academic year	
Assessment Results	Master signed copy held by Academic Registry and electronic copy held in Student Record System permanently 6 months after assessment board for all other copies	

Type Personal Information	Suggested Retention Period	Reasons
Examination Scripts and coursework	<p>1 (calendar) year from date of appropriate assessment board.</p> <p>For 3rd year students going into honours year the Honours Assessment Board is the relevant board (i.e. 3rd year assessments would be kept for 2 years for those students undertaking Honours</p> <p>Professional/statutory bodies may require longer retention</p>	The University Assessment Regulations and Assessment and Graduation Processes, Section 2 Appendices, Appendix 10 Policy on Retention of Student's Work
Personal information of any sort on a web page/site.	No longer than a period specifically agreed with the person.	Danger of inaccurate and irrelevant processing.
Accident books and records and reports of accidents	3 years after the date of the last entry.	RIDDOR 1995
Contact details kept on personal files (e.g., card index, MS Outlook)	Until it is apparent that the person is no longer at the named location.	It is inaccurate processing if the information is held any longer.

Appendix D Photography & the Data Protection Act (1998)

Notes

- (a) As the Data Protection Act (1998) was not drafted to cover specific circumstances and because (as yet) it has not been tested in court, it is not known how perceived breaches of the law will be legally interpreted. With this in mind, these procedures, which were written in conjunction with the University's Information Strategy Manager, should be regarded as general guidelines for good practice in the production and processing of photographic images rather than definitive points of law. They have, however, been drafted with the intention of erring on the side of caution where any doubts arise, in the hope that, should a complaint be filed against the institution, we can demonstrate that we are acting in good faith.
- (b) An official GCU Consent Form has been developed by PDS in conjunction with the University Information Manager for the purpose of obtaining subjects' consent to publish any image in which they might appear. [Can be found at the end of this Appendix]
- (c) Under the terms of the Data Protection Act (1998) photographs featuring pictures of people and any Consent Forms which accompany them are considered to contain personal information and, as such, should be stored securely.
- (d) The terms "published" and "publication" as used below, refer to both printed and electronic media (including web sites, TV and video).
- (e) If in doubt about how to apply these procedures to any specific situation involving the production or processing of photographic images, err on the side of caution or consult the University Information Strategy Manager, Pat McKay (x1450) for guidance before going ahead.

Commissioning New Photography

- Everyone who agrees to appear in a photograph commissioned by the University, should provide their express (written) consent to publish, via the official Consent Form, before the photoshoot begins. They must be fully informed of the consequences of giving their consent (e.g. that this information may be available to countries where their personal information is not protected by law)
- For shoots involving a number of different individuals and/or a number of different shots, an accurate note should be kept of who appears in each photograph, to allow the Consent Forms to be matched up to the appropriate images after the photographs have been processed.
- If the photography is taken in a tangible (i.e. non-digital) format, Consent Forms should be stored with the image to which they refer. If the photography is taken in a digital format, Consent Forms should be stored with a printout of the image to which they refer.
- If a subject appears in more than one photo at a shoot, copies of the Consent Form should be kept with each photo in which the subject appears.
- For photographs containing more than one subject, Consent Forms for all those featured should be stored with the photo to which they refer.
- Photographs may only be published in accordance with the conditions agreed by the subject in providing their express (written) consent.
- Photographs cannot be published if the appropriate Consent Forms are lost or mislaid.
- Exceptions:
 - Where protocol dictates that it would be inappropriate to ask subjects to complete a form:
 - Celebrities and dignitaries will generally expect their photos to be taken and published and should not be asked to complete a Consent Form.

- For visiting academics and guests of the University a quick explanation along the lines of “Do you mind if we take your picture for our publicity material?” will suffice.
- For events involving very large groups (Graduation Ceremonies, launches, etc.):
 - The inclusion of a note within the general documentation sent out to participants to the effect that photographs will be taken at the event for the purposes of publicising the University around the World should ensure that we are covered.
- If shots might include passers-by who are unaware that a photograph is being taken:
 - A notice should be displayed on location reading “Glasgow Caledonian University: Official Photoshoot. These images will be used to publicise the University around the world.” It is important that this wording is used.
- Shots including pictures of children (under 16 years):
 - For events such as Open Day the procedure for events involving very large groups should be followed.
 - For specific pictures in which children are featured, express consent (in the form of a completed Consent Form) must be provided by the child’s parents/guardians or by their school (depending on which is acting as the point of contact).
 - For specific pictures in which pre-school children are featured, express consent (in the form of a completed Consent Form) must be provided by the child’s parents/guardians.

Working with Images for which we do not have Express (Written) Consent to Publish

While consent to publish has been obtained for all the most recent photography commissioned by the University, it is unlikely that it was sought with regard to images created prior to the introduction of the Data Protection Act (1998). If working with images for which we do not have consent to publish, the following procedures should be followed:

- If the subjects were aware that their photo was being taken at the time:
 - Images **can** be used to update an **existing** publication or series of publications in which they have already appeared.
 - Images **cannot** be used in **new** publications unless the subjects cannot be identified. *e.g. at a small scale, blurred, silhouetted, etc.*
- If the subjects were unaware that their photo was being taken:
 - Images **cannot** be used in **any** publication unless the subjects cannot be identified. *e.g. at a small scale, blurred, silhouetted, etc.*
- If the images feature pictures of children (under 16 years) for which we do **not** have express (written) consent to publish:
 - Images **cannot** be used in **any** publication unless the subjects cannot be identified. *e.g. at a small scale, blurred, silhouetted, etc.*

Adam Piggot
Print Design Services
10 November 2003

The Design Team, Print Design Services, Glasgow Caledonian University

Permission to Publish Photographic Images: Consent Form

Section 1

To be completed by anyone appearing in photography for publication by Glasgow Caledonian University

- How the photographs will be used

The photograph(s) in which you have agreed to appear will be used solely to promote the activities of Glasgow Caledonian University and will be held without limit of time. They may be used in printed and electronic form, and may appear in different publications (including web sites, television and large scale exhibition panels), within the UK and overseas, including countries outwith the European Economic Area.

- The Data Protection Act 1998

Under the terms of the Data Protection Act 1998, we need your permission to publish any photographs in which you feature.

- Consent

Please provide the information requested below, giving us your permission to use any images (or parts of images) in which you appear as a result of this photoshoot, in accordance with the conditions outlined above and the terms of the Data Protection Act 1998.

Name (Please Print) Signature Date

Department or Programme

Section 2

To be completed by anyone arranging photography for publication by Glasgow Caledonian University

The University can only publish images which are accompanied by the correct consent form(s). To ensure that this form is linked to the correct image(s), it is important that we are able to identify the individual to which it applies, in any photograph(s) in which they may appear. Please provide a brief objective description (e.g. gender, hair colour, clothes) to help ensure that this can be done.

_____ *Continue on the reverse of this form if necessary*

Location of Photoshoot Date of Photoshoot

The Design Team, Print Design Services, Glasgow Caledonian University

Permission to Publish Photographic Images: Consent Form

Section 1

To be completed by anyone appearing in photography for publication by Glasgow Caledonian University

- How the photographs will be used

The photograph(s) in which you have agreed to appear will be used solely to promote the activities of Glasgow Caledonian University and will be held without limit of time. They may be used in printed and electronic form, and may appear in different publications (including web sites, television and large scale exhibition panels), within the UK and overseas, including countries outwith the European Economic Area.

- The Data Protection Act 1998

Under the terms of the Data Protection Act 1998, we need your permission to publish any photographs in which you feature.

- Consent

Please provide the information requested below, giving us your permission to use any images (or parts of images) in which you appear as a result of this photoshoot, in accordance with the conditions outlined above and the terms of the Data Protection Act 1998.

Name (Please Print) Signature Date

Department or Programme

Section 2

To be completed by anyone arranging photography for publication by Glasgow Caledonian University

The University can only publish images which are accompanied by the correct consent form(s). To ensure that this form is linked to the correct image(s), it is important that we are able to identify the individual to which it applies, in any photograph(s) in which they may appear. Please provide a brief objective description (e.g. gender, hair colour, clothes) to help ensure that this can be done.

_____ *Continue on the reverse of this form if necessary*

Location of Photoshoot Date of Photoshoot

Appendix E Typical documentation for Requests for personal information from the Police

The document below is an example of the documentation that should be produced by the Police when they are seeking personal information about University staff or students. The production of such a form does not automatically mean the information will be released.

Association of Chief Police Officers Code of Practice for personal data requests

DECLARATION FORM FOR DATA USER

NAME OF POLICE FORCE

THIS REQUEST FOR INFORMATION SHOULD BE TREATED AS CONFIDENTIAL.

To:
.....
.....
.....

Data Protection Act, 1984, Section 28(3)

I am making enquiries for the purpose(s) of:-

- * (a) the prevention or detection of crime
- * (b) the apprehension or prosecution of offenders

Nature of enquiry:

The information sought is needed to
.....

I confirm that the personal data requested are required for that/those purpose(s) and failure to provide the information will, in my view, be likely to prejudice that/those purpose(s).

Signed Rank

Name Date
(Block Capitals)

Police Station

Countersigned Rank
(Where necessary)

* Delete as **appropriate**

One copy to the Data User, retained in accordance with force policy.

Appendix F Guidelines for writing references for students

This information has been extracted from the Guideline, prepared by Queen Mary and Westfield College, London, setting out principles for writing references which was made available to the sector by Professor G Zellick and distributed by CVCP (23/09/96)

1. Introduction

- 1.1 A House of Lords decision [*Spring v Guardian Assurance (1994) All England Law Reports 129*] ruled that the author of a reference owes a duty of care to the person about whom it is written, and may be liable in damages to that person if loss is caused through negligence. Hitherto it had been thought that there would be liability only in defamation, and then only if it could be proved that the writer was motivated by malice. Liability may now come about through carelessness either as to matters of fact or in the formulation of opinion. The author of a reference has therefore an obligation to the subject of the reference. The House of Lords did not consider whether the author also has an obligation to the *recipient* of the reference, although such a liability is likely.
- 1.2 These guidelines are intended to provide some assistance in the preparation of references, particularly student references.
- 1.3 The principal aims of a reference are to
 - confirm facts - to confirm the accuracy of the statements made in an application: e.g. qualifications gained, subjects studied, employment dates, work undertaken
 - provide opinions - to give the referee's opinion as to the candidate's suitability for the post/course in question, and his/her potential for the future.
- 1.4 A reference relies on both facts and opinions, and these two should be clearly differentiated.

2. Guidelines

[The following recommended guidelines relate specifically to student references, but the principles are equally applicable to all references]

- 2.1 Students should be told if there is a departmental policy on references. E.g. whether they can assume their adviser will automatically provide a reference if his/her name is cited in an application, or whether s/he should first be approached for permission.
- 2.2 Remember when writing a reference for a student they can ask the requesting organisation for a copy. Under the Data Protection Act the organisation would have difficulty in not providing the student with a copy.
- 2.3 Try to be fair to both the student and the recipient of the reference.
- 2.4 Ensure that the reference is factually accurate and complete – your Programme Administrator can provide you with a printout of the student's programme history, including their transcript from the Student Record System to enable you to check that you have the full information.
- 2.5 Make sure that your opinions are clearly stated as opinions, are based on fact and that you are qualified to give such opinions.
 - Do not confuse fact and opinion e.g. "*on her performance to date, I would be surprised if X did not get a first class degree*" is clearly an opinion; "*she will get a first class degree*" suggests that the method of classification for Honours is such that the issue is beyond doubt.
 - Ensure that the opinions you state are honest opinions based on facts known to you. Do not make statements which you are not qualified to make. E.g. "*I consider X to be well suited to the post for which s/he has applied, and am happy to support his/her*

applications" is better than "X will be a success in the post of..."

- Particular care should be taken where you are asked for a reference for a student who is not known to you (e.g., if the student's adviser is absent, or has left the University). Do not give an opinion which is not your own, just because the person who knew the student has left. It is preferable to quote someone who has knowledge of the candidate, giving the source of the quote.
 - There may be issues on which you are asked to express an opinion on which you have limited knowledge - e.g. honesty and integrity. Here you may have to say, for example, "...I know of nothing that would lead me to question X's honesty"
- 2.6 Avoid using ambiguous or 'coded' language. e.g., "X has studied here for three years, during which time he has done his work entirely to his own satisfaction".
- 2.7 If the reference asks for information on the health or medical history of the student you must get the students **explicit** consent to mention these matters. A student asking you to provide a reference for them is **not** sufficient.

3. Other

3.1 Telephone references:

The same guidelines apply to references given over the telephone. Do not be tempted to make incautious statements simply because they are not in writing. Ideally, references should not be given over the telephone (you do not know how the information will be filtered as it passes through the various stages of what the enquirer understood you to say; what s/he jotted down; what s/he reported orally to the panel). Limit the information you provide to facts and follow up immediately with an email, letter or Fax.

- 3.2 *Unsolicited reference* (i.e. for a person who has not, to your knowledge, cited your name as a referee) Pass these to Academic Registry who will send a response asking for the organisation to provide the University with consent from the student.

Appendix G

Standard Request Form for Access to Personal Data (Student)

Name (*Block letters*) _____

Address _____

Date of Birth _____

Programme of Study _____

Year _____

Matriculation Number _____

I wish to have access to the following personal data that Glasgow Caledonian University holds about me:

Please specify where you think this information is held:

I understand that before the above information can be disclosed I will be required to produce my Matriculation Card as means of identity.

Signed: _____

Date: _____

Send the completed form and a £10 fee (cheque made payable to Glasgow Caledonian University) to *Head of Information Strategy Unit, Glasgow Caledonian University, Cowcaddens Road, Glasgow G4 0BA.*

Appendix H

Standard Request Form for Access to Personal Data (Staff)

Name (*Block letters*) _____

Address _____

Staff Card number _____

Department _____

I wish to have access to the following personal data that Glasgow Caledonian University holds about me:

Please specify where you think this information is held:

I understand that before the above information can be disclosed I will be required to produce my Staff Card as means of identity.

Signed: _____ *Date:* _____

Send the completed form and a £10 fee (cheque made payable to Glasgow Caledonian University) to *Head of Information Strategy Unit, Glasgow Caledonian University, Cowcaddens Road, Glasgow G4 0BA.*