



University
of Worcester

**DATA PROTECTION CODE OF
PRACTICE**

CONTENTS

Glossary of Terms	1
Introduction	2
Key Concepts and Principles	2
Transfer of Data to Third Parties	3
Security of Personal Data	4
Examinations	6
Confidential References	7
Transfer of Personal Data to Non-EEA Countries	7
The Internet and World-wide Web	8
Staff and Student Directories	9
Collection of Personal Data Via the Web	9
Arrangement for the Collection and Storage of Sensitive Data	10
Emergency Contact Information	10
Alumni Records	10
CCTV	11
Photographic Images in Publications	11
Publicity and Press Releases	11
Information to Staff and Students	11
Subject Access Requests	11
 <u>Appendices</u>	
Employee Access to, and use of, Personal Data	Appendix 1
Student Access to, and use of, Personal Data	Appendix 2
The Eight Data Protection Principles	Appendix 3
Access Request Form	Appendix 4



DATA PROTECTION CODE OF PRACTICE

Glossary of Terms

- Data Controller:** is the organisation which must determine the purposes for which, and the manner in which, any personal data are processed.
- Data Subject:** an identifiable or identified living individual who is the subject of the personal data
- Personal Data:** data which relates to a living individual who can be identified from that data.

Sensitive Personal

- Data:** some personal data is known as “sensitive personal data” and is subject to special rules. The Act defines sensitive personal data as:-
- a) the racial or ethnic origin of the data subject;
 - b) his political opinions;
 - c) his religious beliefs or other beliefs of a similar nature;
 - d) whether he is a member of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992);
 - e) his physical or mental health or condition;
 - f) his sexual life;
 - g) the commission or alleged commission by him of any offence or
 - h) any proceedings for any offence committed or alleged to have been committed by him, the disposal of such proceedings and the sentence of court in such proceedings.
- [Section 2, 1998 Act]

Relevant filing System:

The term “relevant filing system” is defined in the Act as:

Any set of information relating to individuals to the extent that, although the information is not processed by means of equipment operating automatically The set is structured, either by reference to individuals or by reference to criteria relating to individuals, in such a way that specific information relating to a particular individual is readily accessible.

Introduction

1. This Code of Practice is based on the JISC Code of Practice for Further and Higher Education in the United Kingdom. The Code has been approved by the University's Information Strategy Group. It is intended to be used to ensure that the institution, its employees and students, collect, store and use data only in ways which comply with the Data Protection Act, 1998.
2. The institution will only process data for the purposes which have been notified under the Data Protection Act (DPA). An audit of data processing activities in the institution will be undertaken on an annual basis.
3. The institution has appointed two Data Controllers:-

Registrar and Secretary (student related data)
Head of Personnel (employee data)

It is the responsibility of the Data Controllers to ensure that the institution complies with the terms of the DPA. General queries relating to the Act and this Code of Practice should be referred to the Registrar.

4. Individual employees must respect the rights of data subjects and their own responsibilities with regard to access to and use of personal data. These are set out in the separate guidelines for staff on the Data Protection Act (Appendix 1 to the Code)
5. In cases where students are processing personal data for which the institution is Data Controller, then the student conducting the research, or engaged in the course of study, can rely on the institution's notification. Students must conform to the guidelines issued to them on their responsibilities under the DPA (Appendix 2 to the Code).

Key Concepts and Principles

6. The first and most basic tenet underlying the provision of the DPA is that of Purposes. Thus, the institution will process personal data only where it has a clear purpose for doing so.

7. There will be many legitimate purposes for the processing of personal data, even where the data subject may not wish this to happen. The essential element is that of ensuring Fairness in the relationship between data controller and data subject. Where required the institution will demonstrate the fairness and legality for any data processing it undertakes.
8. The final element of the data protection regime is Transparency and the institution will take all steps to ensure that data subjects know the purpose of the processing and the measures that have been taken to ensure that the processing is fair.
9. The Principles in the Data Protection Act, 1998, are set out at Appendix 3.

Transfer of Data to Third Parties

10. The institution will ensure that personal data under its control is not disclosed to unauthorised third parties. Unauthorised third parties will include: family members, friends, local authorities, government bodies, and the police, unless disclosure is exempted by the 1998 Act, or by other legislation. In all other cases the consent of the data subject will be sought.
11. Data may be disclosed to third parties without consent of the individual where it is required for the:-
 - purpose of protecting the vital interests of the data subject (i.e.: release of medical data where failure to release data would result in harm to, or the death of, the data subject);
 - purpose of preventing serious harm to a third party would occur if the data were not disclosed;
 - purpose of safeguarding national security;
 - prevention or detection of crime
 - apprehension or prosecution of offenders;
 - assessment or collection of any tax or duty or of any imposition of a similar nature;
 - discharge of regulatory functions, including securing the health, safety and welfare of persons at work.
12. Data may also be disclosed to third parties without consent where:-
 - it is to be used for research purposes, subject to the rules relating to use of personal data in research
 - it is information which the institution is obliged by legislation to provide to the public,

- where the disclosure is required by legislation, by rule of law or by the order of a court (ie HE and FE institutions' are legally obliged by the Higher Education Statistics Agency to collect first destination data for graduating students).
13. Staff will ask to see official documentation in support of a request for information about a data subject. The absence of such documentation or a warrant may justify refusal to disclose the requests personal data. In cases of doubt, the advice of the Data Controller(s) should be sought.
 14. Although details about a student will normally be passed to employment agencies or prospective employers, care must be taken to ensure that the third party has a genuine requirement for the information. Telephone disclosure will not be permitted.
 15. In all other cases, measures will be taken to ensure that personal data is not inadvertently disclosed to unauthorised third parties (which shall include parents and relatives, Embassies and High Commissions). If a request for information is refused, but the subject matter of the enquiry is evidently of interest and/or importance to the data subject, they should be informed of the enquiry. This shall normally be achieved by forwarding the request to the student's last-recorded address. Where the matter appears urgent, an attempt will be made to contact the student by telephone or other means in order to put him or her in touch with the enquirer.
 16. Third parties claiming the right to access a data subject's personal data under any of the exemptions described above should be required:-
 - to provide reasonable proof of their personal identity and organisational affiliation according to the circumstances of the request and the nature of the personal data requested;
 - to submit a request to the appropriate person. Requests for personal data by police officers should be supported by warrant, or by suitable paperwork provided by the local force stating that the information is required in support of an ongoing investigation.
 - where reasonable, to provide a written and signed document to the institution containing: the purpose for which the data is being requested; the time for which it is to be held; and a warranty that it will be held and processed in conformity with the Data Protection Principles.

Security of Personal Data

17. Staff with access to computerised and manual systems which contain personal data will take all reasonable steps to ensure that it is secure. The basic principles of security of computer-held personal data are set out

in separate guidelines, "Regulations for the use of IT facilities by staff and students." Staff with responsibility for manual files which contain personal data should ensure that filing cabinets are secure and that office doors are locked during staff absences. Filing cabinets should conform to minimum levels of fire protection.

- 18.** In cases where vendors, contractors and suppliers are required to have access to areas in which personal data may be stored or processed, such persons shall be:
 - registered and required to wear some form of identification
 - restricted from unnecessary admittance to areas where personal data is held or processed
 - required to sign non-disclosure agreements where access to personal data is unavoidable.
- 19.** Employees (and students) are advised to challenge, or report to security, individuals without proper authorisation found in areas where personal data is held or processed.
- 20.** Reasonable precaution must be taken when transferring personal data, whether in hardcopy or electronic form. Information containing personal data, and in particular sensitive personal data, which is to be transferred by electronic means (e.g. e-mail, WWW, FTP) should be encrypted before transmission. Personal data sent in hardcopy should be transferred in a manner appropriate to its sensitivity (e.g. in sealed envelope, or by hand in certain circumstances)
- 21.** Employees (and students) must take particular care when processing personal data at home or in other locations (e.g. in public places or on public transport) outside the institution. They must ensure that:-
 - they take reasonable precautions to ensure that the data is not accessed, disclosed or destroyed as a result of act or omission on their part.
 - they ensure personal data held in manual form is stored as securely as possible, and ideally is locked away when not in use.
 - they have an up-to-date virus-scanning program installed on laptop computers or personal machines and scan all disks, e-mails, and other potential virus vectors for viruses.
 - they back up system hard drives to avoid loss of data
 - they report all computer security incidents including virus infections to the institution
- 22.** When using a laptop to process personal data for which the institution is Data Controller they must ensure that they;-

- keep the laptop constantly in view when travelling, especially in busy places;
 - do not check the laptop as baggage unless it is placed inside luggage that has been locked
 - record the model number and serial number of each hardware component associated with the laptop and keep this information in a separate location
 - notify the institution immediately in the event of loss or theft.
- 23.** The proper disposal of personal data is the responsibility of all staff (and students) who have a responsibility for the security of personal data. Failure to dispose of data properly will be a disciplinary offence. Data will be disposed as follows:-
- the minimum standard for the destruction of paper and microfilm documentation should be shredding
 - paper and microfilm documentation containing sensitive personal data should be shredded or incinerated
 - the minimum standard for the destruction of data stored in electronic form should be reformatting or overwriting
 - electronic storage media containing sensitive personal data should be destroyed
- 24.** Where disposal of equipment or media is contracted to a third party, the contract shall require the third party to ensure that all personal data is completely destroyed. The contract shall permit the institution to audit the third party's performance of this term at regular intervals.

Examinations

- 25.** While examination scripts are exempted from the data subject access rules, the institution will ensure that data subjects are allowed access to the following within the stipulated timescale, unless the data cannot be disclosed without additionally disclosing personal data about a third party:
- Internal examiners' comments
 - External examiners comments
 - Examination board minutes and related documentation

The limit for meeting the request of the data subject is normally 40 days, but in the case of examinations the DPA specifically notes that a request may be made before results are announced. In this case there is a limit of five months from the request or 40 days from the announcement, whichever is the earlier.

26. Each programme of study shall, where appropriate, produce;-
- a formal statement that explains the logic behind any assessment that is based entirely on automated means, including single tests that form only a part of some larger assessment;
 - a formal statement that explains the logic behind any classification or grading system that operates using automated means
27. All steps will be taken to ensure that the results of students are not disclosed to third parties without the data subject's consent. Students will be informed that the names of successful students will be included in pass lists published within the institution, in awards ceremony brochures, and in local newspapers on the date of each awards ceremony. Data subjects will be able to exercise their right to object to their results being displayed in all or any particular form.
28. The results of individual students will be made available via secure electronic means (password protected) and via the post. In the absence of specific consent from the data subject results will not be disclosed to any other individual. Results will only be given over the telephone when the caller has satisfactorily answered at least two security questions (e.g.: student number and date of birth).

Confidential References

29. Under the Data Protection Act 1998, a data subject may request access to any personal data held by the University. This includes personal references held on file for students and employees. In the event of a request being made by any person for whom the University College holds a reference, the permission of the person who provided a reference will be needed. All requests for references will be asked to consent to disclosure. Anyone refusing consent will be asked to state their reasons. If a referee declines consent a judgement would be made at the time of a subject access request on the available information. Efforts would be made to ensure anonymity.
30. Whilst confidential references given by HE institutions are exempted from subject access requests and institutions have the absolute discretion to refuse to release confidential references written on behalf of its employees and students, UCW will allow access to personal references held on file in the event of a subject access request by an employee or student. This principle will apply equally to references provided for internal as well as external purposes.

Transfer of Personal Data to Non-EEA Countries

31. Personal data shall not be transferred to a country or territory outside the European Economic Area (the EU Members States, plus Norway, Iceland and Liechtenstein) unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data. In considering the transfer of data to non-EEA countries, UCW will rely on the guidance produced by the Office of the Information Commissioner titled, "The Eighth Data Protection Principle and Transborder Dataflows".
32. Where the data subject has given consent to transfer, personal data may be transferred to a non-EEA country without an adequate level of protection.
33. Circumstances where transfer of personal data to a non-EEA country may be necessary include:-
 - requests to non-EEA governments, agencies and organisations for information necessary to determine academic eligibility for attending a course of study at the institution.
 - transfers of personal data to non-EEA governments, agencies and organisations sponsoring students to attend a course of study where sponsorship is dependent upon attendance and/or performance criteria.
 - transfers of personal information (e.g.: examination marks) relating to and required by data subjects engaged in distance learning courses, exchange programmes and placements abroad (staff and student).
34. In all other circumstances, the institution will obtain the written and informed consent of the data subject before transferring personal data to a non-EEA country, except where a data subject requests a reference be written and sent to a non-EEA country, when the request itself will indicate their consent to the transfer.
35. UCW will not in the absence of a sponsorship arrangement, disclose personal data for the purposes of assessing the names, numbers and whereabouts of foreign nationals studying or working at the institution, without the specific and informed consent of the data subjects concerned.

The Internet and World-wide Web

36. UCW will use non-sensitive staff personal data (e.g.: name, position held, research interests, academic qualifications) on its Internet and Intranet web pages without consent where:

- its display facilitates the normal organisational functioning and management of the institution. The information displayed will normally be the same as that available in hardcopy publications.
 - staff are informed that certain personal data will be displayed on institutional web pages, and have the right to object to the use of their data where it would cause them significant damage or distress. Retaining the right to object does not mean automatically being able to have data removed. The institution will make a judgement, on the basis of the data subject's objections, on whether the damage or distress alleged is a suitable ground for removal.
- 37.** Staff will be made aware of which of their personal data will be displayed at the point they take up post and given an opportunity to object. The right to object will apply at any time and staff will receive an annual reminder of their right.
- 38.** The University will not use sensitive staff or student personal data on institutional web pages without explicit consent.

Staff and Student Directories

- 39.** The institution will include staff telephone and e-mail directories on its Internet web site where :
- these facilitate the normal organisational functioning and management of the institution
 - staff are informed as appropriate and reminded annually that certain personal data will be included in such directories and have the right to object at any time to the use of their data where it would cause them significant damage or distress.
- 40.** The University will include student telephone and email directories on restricted access Intranets where:
- these facilitate the normal organisational functioning and management of the institution
 - students are informed at point of entry that certain personal data will be included in such directories and have the right to object at any time to the use of their data where it would cause them significant damage or distress.
- 41.** Consent from students will be sought before their data is included in on-line email directories available on the institution's Internet website and students will be able to opt out of having their details displayed.

Collection of Personal Data Via the Web

42. In all cases where personal data is collected via web pages (e.g.: prospectus requests, potential student and employee applications), the University will inform the data subject of:-
- the purpose for which the data is collected
 - the period for which the data will be provided (e.g.: “while we process your applications”, “for the duration of your studies”.)
43. The data subject will be provided with the facility to opt out of any parts of the collection or use of the data that are not directly relevant to the transaction (e.g.: where an individual provides their name and address to obtain a prospectus and it is intended to follow up with a communication to discover why candidates did not come to the institution, the individual will be notified and be able to opt out).
44. In the event of a subsequent decision to use the data for a purpose which was not disclosed at the point of collection, further consent will be obtained from the data subject.

Arrangements for the Collection and Storage of Sensitive Data

45. The University recognises the importance of stringent arrangements to control the collection and storage of sensitive personal data. Some services will, inevitably, need to collect and retain data of a personal and sensitive nature, in particular:-
- Registry
 - Personnel
 - Student Services (and especially the Medical Centre, Counselling Service, Financial Advisory Service and Careers Service)
 - Equal Opportunities Centre

Each of the above areas will produce a specific Data Protection Statement.

Emergency Contact Information

46. The institution will hold records for its staff and students for use in emergency situations. The consent of the individual or individuals to be contacted in case of emergency will not be sought but:-
- staff and students are advised via the collection form that the emergency contact data will only be used for emergency purposes;

- the emergency contact data will only be disclosed in emergency situations in the immediate health or safety interests of the staff member or student;
- staff and students are advised via the collection form that they should notify the individual or individuals to be contacted of the disclosure to the institution of the individual's or individuals' details;
- obtaining the consent of the individual or individuals to be contacted would involve disproportionate effort.

Alumni Records

47. The institution will maintain a database of alumni records and will ensure that:-
- students are informed at the time of the collection of their personal data for an alumni database of the purpose of that collection;
 - students and alumni are given an opportunity to opt out of the collection and processing of their personal data, at the point of the completion of their course of study and subsequently on an annual basis;
 - students and alumni are able to request that where their personal data are collected and processed for alumni contact purposes, the data are not also processed for direct marketing purposes (e.g.: advertising inserts in the alumni magazine);
 - alumni are given an opportunity, on an annual basis, to update their record or to have it removed from the database.

CCTV

48. The University will follow the guidance in the "Code of Practice for users of CCTV and similar surveillance equipment monitoring spaces to which the public have access".

Photographic Images in Publications

49. The institution will seek the agreement of any person whose photographic image is to be used in any form of publication which includes recruitment materials and newsheets and magazines

Publicity and Press Releases

50. Occasionally, the institution will wish to issue information to the press which may include personal data. The permission of the data subject will always be sought before information is released.

Information to Staff and Students

51. The staff contract will include reference to Data Protection arrangements and in accepting an appointment, individual staff will sign a declaration that they have read and understand the institution's Data Protection Policy.
52. At registration, students will receive a statement on Data Protection and will sign a statement that they understand it.

Subject Access Requests

53. Data subjects may request access to the personal data which the institution holds on them by application on the relevant form and after payment of the £10.00 fee. Members of staff should submit their application to the Personnel Department, students should apply to the Registry. A copy of the access request form is attached at Appendix 4.

John Ryan
Registrar and Secretary to the Board of Governors

DATA PROTECTION CODE OF PRACTICE: EMPLOYEE ACCESS TO, AND USE OF, PERSONAL DATA

1. Staff are reminded that all personal data collected, held, and processed are subject to the Data Protection Principles contained in the Data Protection Act, 1998
2. This responsibility extends to data which is held on computers as well as in structured manual files.
3. As part of their training and induction staff will be made aware of the circumstances in which these may, as a legitimate part of their employment, access, process and disclose personal data.
4. Staff should only process personal data for which the institution is Data Controller and for a purpose which must be explicit, valid and covered by the institution's notification under the Act.
5. Compliance with the Data Protection Code of Practice is a condition of employment at the University of Worcester and it is the individual staff's responsibility to ensure that they are familiar with the content of the Code and that they attend briefing sessions as required. Staff who contravene the Code of Practice may be subject to disciplinary action.
6. Subject access to data held about them is a fundamental principle established by the Act. Where individual member of staff receive requests for access to data for which they have a responsibility, they must ensure that the proper procedure is followed.
7. Where staff are uncertain about any aspect of the collection and processing of data, they should consult one of the Institution's two Data Protection Officers:-

For student data: John Ryan
Registrar and Secretary
j.ryan@worc.ac.uk
(01905) 855015

For staff data: Gillian Slater
Head of Personnel
g.slater@worc.ac.uk
(01905) 855443

DATA PROTECTION CODE OF PRACTICE: STUDENT ACCESS TO, AND USE OF, PERSONAL DATA

1. The Institution's notification under the Data Protection Act 1998, includes the collection of personal data for the purpose of research. Where students are conducting research, or engaged in a course of study, and this requires them to collect and process personal data, they can rely upon the institution's notification.
2. Students must ensure that they observe the rules for the collection and processing of personal data, particularly in the case of possible transmission to unauthorised third parties. The importance of compliance with the principles of the Data Protection Act should be covered in relevant induction and training courses, especially for research students and for students undertaking independent studies.
3. In some cases, students may be involved in collection and processing sensitive personal data, and in these circumstances it will be especially important to ensure that compliance with the Act is maintained. Students should consider these issues in formulating proposals and should read appropriate guidelines carefully and make application to the Ethics Committee as appropriate.
4. Where students process data for their own personal or domestic use the Institution is not responsible for including such use in its notification or for ensuring that the processing complies with the Data Protection Principles.
5. There may be occasions when students may have to notify the Data Protection Commission themselves, but these occasions will be rare, and normally only where they either fall outside the institutional notification or the "personal or domestic purposes" exception. In most cases, this is likely to involve the processing of data intended to lead to the commercial exploitation of personal data.
6. Students may, on occasion, have access to personal data held and processed with the University, e.g.: during periods of part-time employment. In such circumstances, students should be aware that, like any other employee, they will be subject to the Code of Practice on Data Protection.

7. Where students are uncertain about any aspect of their involvement in the collection and processing of personal data they should consult the institution's Data Protection Controller for Student data:-

John Ryan
Registrar
j.ryan@worc.ac.uk
(01905) 855014

DATA PROTECTION CODE OF PRACTICE: THE EIGHT DATA PROTECTION PRINCIPLES

1. Personal data shall be processed fairly and lawfully.
2. Personal data shall be obtained only for one or more specified and lawful purpose, and shall not be further processed in any manner incompatible with that purpose or those purposes.
3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
4. Personal data shall be accurate and, where necessary, kept up to date.
5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.
6. Personal data shall be processed in accordance with the rights of data subjects under the Act.
7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
8. Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.



DATA PROTECTION SUBJECT ACCESS REQUEST FORM
(For use by staff and students)

Students: Please return the form to the Registrar and Secretary
Staff: Please return the form to the Head of Personnel

<p>1. Details of person requesting the information</p> <p>Full Name</p> <p>Student Number (where appropriate)</p> <p>Address</p> <p>.....</p> <p>Tel No Fax No</p> <p>Email</p>
<p>2. Are you the data subject?</p> <p>YES: If you are the Data Subject please supply evidence of your identify i.e.: photocopy of birth certificate, driving licence or passport and a stamped addressed envelope for returning the document to you.</p> <p>NO: Are you acting on behalf of the Data Subject with their written authority? If so, that authority must be enclosed (Please complete question 3 and 4)</p>
<p>3. Details of the Data Subject (if different to 1)</p> <p>Full Name</p> <p>Address</p> <p>.....</p> <p>Tel No Fax No.....</p> <p>Email</p>

4. Please describe your relationship with the Data Subject that leads you to make this request for information on their behalf.

.....
.....

5. Please describe the information you seek together with any other relevant information. This will help to identify the information you require. You should include details of the period covered by the request, the location of the data you seek (for example, central student/staff file; departmental file; email correspondence, etc) *Please continue on a separate sheet if necessary.*

.....
.....
.....

The University is allowed to charge for each application. The current fee is £10.

Declaration: To be completed by all applicants. Please note that any attempt to mislead may result in prosecution.

I, certify that the information given on this application form to the University of Worcester is true. I understand that it is necessary for the Institution to confirm my/data Subject's identity and it may be necessary to obtain more detailed information in order to locate the correct information.

Note: The period of 40 days in which the organisation must respond to the request will not commence until it is satisfied upon these matters.

Signature

Date

Signature of the data subject if they are not the person requesting the information:

Please return the completed form to The Registrar and Secretary or Head of Personnel, University of Worcester, Henwick Grove, Worcester, WR2 6AJ.