

Data Protection Policy

1. Introduction

- 1.1 The Data Protection Act 1998 (“the Act”) gives rights to individuals, including staff and students, about whom information or “personal data” is obtained or processed. This Policy does not distinguish between manual and electronic processing of data.
- 1.2 This Policy summarises and explains the legal obligations placed upon the University of Chichester (the “University”) with regard to its data processing activities.
- 1.3 The University is fully committed to complying with its obligations under the Act, in respect of all processing of personal data in connection with its business and in so doing meeting the expectations of its staff and students.
- 1.4 A “data subject” is any individual about whom the University processes personal and/or sensitive personal data.
- 1.5 “Staff”, “students” and “other data subjects” may include past, present and potential members of those groups. “Other data subjects” and “third parties” may include contractors, suppliers, contacts, referees, friends, family members, or any other person that the University conducts its business with.

2. What is Personal Data?

- 2.1 Personal data is information which relates to a living individual (ie not companies) who can be identified from that information, (whether directly or indirectly on its own or in conjunction with any other information held).
- 2.2 Personal data must relate to that individual’s personal, private, business or professional life. Examples of personal data that the University may process from time to time in its day to day business are detailed in Appendix 1.

3. What is processing?

- 3.1 Data processing is the collective term for any action or operation carried out in relation to personal data. This includes collection, use, transfer, download, amendment, storage, deletion and retention of personal data by the University, amongst other tasks.
- 3.2 The purposes for which personal data is processed by the University are set out in Appendix 2 to this Policy. If the University processes personal data for new or amended purposes, it will update this Policy to notify staff, students and other data subjects accordingly.
- 3.3 As a result, the University recommends that staff, students and other data subjects check this Policy regularly to ensure that they are aware of the latest version and any relevant changes from time to time.

4. Sensitive Personal Data

- 4.1 Sensitive personal data is personal data relating to:
 - race;

- political opinions;
 - health (physical or mental);
 - religious beliefs;
 - trade union membership;
 - criminal records and alleged offences;
 - racial or ethnic origin;
 - sexual life.
- 4.2 The University may, in some circumstances, be obliged by law to process sensitive personal data about a data subject. For example, some jobs or courses will bring the applicants into contact with children, including young people between the ages of 16 and 18, and the University has a duty under the Children Act 1989 and other enactments to ensure that staff are suitable for the job, and students for the courses offered by making certain criminal checks. The University may also require such information for the administration of the sick pay policy, the absence policy or the equal opportunities policy, or for academic assessment.
- 4.3 There are additional legal requirements placed upon the University where it is processing sensitive personal data. In some cases the University requires the explicit consent of the data subject before processing any of his/her data. Students may provide their consent at the time of acceptance of a course; staff may provide their consent at the time of employment by signing an explicit notice of consent.
- 4.4 The University also asks for information about particular health needs, such as allergies to particular forms of medication, or conditions such as asthma or diabetes. The University will only use such information where legally permitted to do so, to protect the health and safety of the individual, for example, in the event of a medical emergency.
- 4.5 In certain limited circumstances, the University does not have to obtain an individual's consent to process his or her sensitive personal data. The circumstances most relevant to the University are:
- the processing is necessary to protect the vital interests of the data subject (where consent cannot be given by the data subject or cannot reasonably be obtained by the University) or of another person (where consent by the data subject has been unreasonably withheld - for example in a medical emergency).
 - the processing relates to information deliberately made public by the data subject;
 - the processing is necessary for an employment related legal (not contractual) obligation;
 - the processing is carried out by a health professional and is necessary for medical purposes; or
 - the data relates to racial or ethnic origin and is processed in the context of equal opportunity monitoring.

5. The Rules for Processing Personal Data

Any personal data shall be processed in accordance with the Data Protection Principles contained in the Act. These are that personal and sensitive personal data must:

- be processed fairly and lawfully;
- be obtained for a specified and lawful purpose and shall not be processed in any manner incompatible with the purpose;
- be adequate, relevant and not excessive for the purpose;
- be accurate and up-to-date;
- not be kept for longer than necessary for the purpose;
- be processed in accordance with the data subject's rights;
- be kept safe from unauthorised processing, and accidental loss, damage or destruction; and
- not be transferred to a country outside the European Economic Area, unless that country has equivalent levels of protection for personal data, except in specified circumstances.

In addition, the University cannot use or process Personal Data unless one or more conditions are met. The conditions most relevant to the University are:

- with (implied) consent from the data subject;
- where necessary to enter a contract with a data subject at their request or to perform a contract with a data subject; or
- where a legitimate business interest which is proportionate (ie not unwarranted bearing in mind the individual rights and freedoms of the data subject).

This overlaps with the University's legal obligations under human rights legislation.

6. Rights of Access to Information

6.1 The University has a central procedure for dealing with all requests for access to personal information, in accordance with the provisions of the Act. A data subject may ask for their own Personal data (a "subject access request"). The Act does not generally permit a person to see Personal Data about other people. Generally, if such a valid subject access request is made the University will (if requested):

- advise the data subject whether it is processing any personal data concerning them (or on their behalf);
- if so, give the data subject a description of that personal data, the purposes for which the data is being processed and the recipient or classes of recipient to whom it is or may be disclosed by the University;
- tell the data subject, in an intelligible and permanent format (unless the cost of such permanent format would be disproportionate), the information contained in that personal data and its source; and

- if relevant, advise the data subject of the logic involved where a decision relating to or significantly affecting the data subject is made on the basis of processing that personal data by automatic means.

6.2 All requests will be dealt with by the Data Protection Officer within 40 days of receipt of the valid request from the individual in writing (unless there is good reason for delay, in which case, this reason will be explained in writing by the Data Protection Officer to the data subject making the request). For a valid request the applicant must clearly identify themselves and their request for their Personal Data and pay a £10.00 access fee made payable to the University. Any requests received by staff must be passed immediately to the Data Protection Officer. The University may defer dealing with a subject access request while it requests (and until it receives) proof of identity of an applicant and/or the £10 fee.

6.3 Staff, students and other data subjects have the right to access personal data that is being processed about them. Any person may exercise this right by submitting a request in writing to the Data Protection Officer in accordance with 6.2 above.

7. Further Data Subject Rights

7.1 In addition to the right of access, every data subject has a right to require that the University corrects or deletes any inaccurate data held about him/her. Any requests for inaccuracies to be corrected should be addressed to the University's Data Protection Officer. The University is not obliged to do so in all cases. In that situation the University will normally note the comments of the data subject in relation to the relevant data.

7.2 If the data subject believes that the University is going to process his or her data in a way that would be damaging or distressing to him or her, (s)he has the right to object to the University processing his/her personal data in that manner. In such circumstances the University will review the data processing which is the subject of the complaint and will stop data processing where required under the Act. It may not have to (or be legally able to) stop all data processing.

7.3 The data subject is entitled, by written notice, to require the University to ensure that no decision which significantly affects that data subject is based solely on the processing by automatic means of the data subject's personal data.

7.4 Any data subject has the right to request the Commissioner to assess whether any provision of the Act has been contravened by the University. This is a serious step which should not be abused and which should not be taken as a last option if matters cannot be reasonably agreed with the University.

8. Data Accuracy

8.1 Personal data must be kept accurate and where necessary up to date. It must be adequate, relevant and not excessive for the purpose it was collected for.

8.2 The University will take reasonable steps to ensure accuracy and quality of personal data, and to prevent it becoming out of date. Staff members and students will receive regular requests to update their personal data and are responsible for doing so promptly and accurately. Staff and students must provide the University with true and accurate data and promptly notify it, where relevant, of any changes to it. Any incorrect or out of date data will be removed as soon as possible.

9. Data Security

9.1 Personal data will be stored and managed securely in compliance with this Policy and the Information Security policies and standards.

9.2 Personal data must be kept and handled securely (both for electronic and paper records) and all staff must take precautions against physical loss or damage occurring to personal data and to minimise unauthorised access. Staff, students and, to the extent, relevant other data subjects must ensure that both access to and disclosure of their personal data is restricted as appropriate. The University expects staff to be responsible for ensuring that appropriate security measures are taken. For example:

- computers are locked at all times when unattended;
- sensible password on blackberries and mobile phones are set;
- passwords are not shared or left unsecured and are changed when required; and
- Sensitive material is treated carefully, stored separately and not left unattended.

9.3 Sensitive personal data must be protected with a higher level of security. It is recommended that sensitive records are kept separately in a locked drawer or filing cabinet, or in a password-protected computer file. Where such information is taken off the main University sites, for example on a memory stick or laptop, this should be with the prior written authority of their supervisor and in accordance with any conditions set, the measure to be taken to safeguard such information should be implemented in accordance with advice from IT and the Data Protection Officer. If a member of staff, or a student, is holding, or intending to hold, sensitive personal information which is outside standard University processing, eg. for a research project, the Data Protection Officer should be notified with details as soon as possible.

9.4 To assist Staff in ensuring they are aware of their responsibilities in this area, the University has prepared a Staff Guidance Policy which contains further guidance for staff in this area. A copy of this policy is contained in Appendix 4.

10. Retention of Data

The University will keep different types of information for different lengths of time, depending on legal, academic, fiscal and operational requirements. The retention periods of the data that the University processes is detailed in Appendix 3.

11. The Data Controller and the Designated Data Controllers

The University is the data controller under the Act, and the Vice Chancellor is ultimately responsible for its implementation. The Data Protection Officer will be responsible for dealing with daily issues.

12. Assessment Marks

Students shall be entitled to information about their marks for assessments; however this may take longer than other information to be provided. The University may withhold enrolment, awards, certificates, accreditation or references until monies or any other financial obligation due to the University have been paid.

13. Compliance

- 13.1 Compliance with the Act generally is the responsibility of all students and members of staff. Any deliberate or reckless breach of this Policy or action which leads to the University being in breach of its obligations under the Act may lead to disciplinary, and where appropriate, legal proceedings.
- 13.2 Any individual, who considers that the Policy has not been followed in respect of personal data about him or herself, should raise the matter with the Data Protection Officer initially. If the matter is not resolved it should be referred to the staff grievance or student complaints procedure.

14. Staff Responsibilities

All staff shall comply with the Staff Guidance Policy a copy of which is annexed to this Policy in Appendix 4.

15. Student Responsibilities

All students shall comply with the guidance contained within Appendix 5.

16. Computer Equipment

Students and staff must comply with the University's policies on use of IT facilities and/or email systems.

17. Other Use

- 17.1 The University receives public funding and accordingly is subject to audit as a matter of law and to comply with the requirements of funding agreements. Such audits may involve processing personal data but are carried out subject to strict legal and/or contractual controls.
- 17.2 The University is sometimes, unfortunately, involved in claims and/or investigations. Personal Data may be processed, where necessary, in relation to crime prevention, national security and/or dealing with legal proceedings or taking legal advice.
- 17.3 The University necessarily works with many partners to operate successfully and in doing so must sometimes subject to strict contractual controls, disclose or share Personal Data with such partners or service providers. In some cases, these partners are in other countries whose laws do not protect personal data or data subject rights as well as our laws. In those cases, your personal data and rights are protected by other means to adequately safeguard them as required by law.

Appendix 1.

Data Processed by the University

Academic Registry

Data Source
Student files/records/academic references: electronic & paper
Student Transcripts (academic): electronic
Student Additional Requirements Agreement (SARA) Forms (re disability): paper
Pass Lists: electronic and paper
Mark Schedules: electronic and paper
Assessment Forms: electronic and paper

Student Services

Data Source
Counselling notes, paper and electronic
Health notes, paper and electronic
Disability assessment notes, paper and electronic
Advice notes, paper and electronic documents
Advice notes, paper and electronic documents
Advice notes, paper and electronic, destinations data

Finance

Data Source
Credit card details student/parents for regular payment plans
Invoices unpaid/paid
Student/Student Loans Company records

Human Resources

Data Source
Staff Record
Unsuccessful job applications
PDRP (Personal Development Record)
Disciplinary Case Investigation notes
Sickness Records
Criminal Records Bureau documentation
Accident at Work Records

Appendix 2

University Information Processing

The University has notified the Information Commissioner that personal information may need to be processed for the following purposes:

- Staff, Agent and Contractor Administration
- Advertising, Marketing, Public Relations, General Advice Services
- Accounts & Records
- Education
- Student and Staff Support Services
- Research
- Other Commercial Services
- Publication of the university magazine
- Alumni relations
- Police/solicitors

Complete details of the University's current entry on the Data Protection Register can be found on the notification section of the [Information Commissioner's web site](#). Select the option to **Search Register** and when the search form is displayed, type University of Chichester into the Name box and then click on **Search**

The register entry provides:

- a fuller explanation of the purposes for which personal information may be used (in broad but not detailed terms)
- details of the types of data subjects about whom personal information may be held
- details of the types of personal information that may be processed
- details of the individuals and organisations that may be recipients of personal information collected by the University
- information about transfers of personal information.

Appendix 3.

Retention Periods (of data processed)

Academic Registry

Data Source	Location	Retention Policy
Student files/records/academic references: electronic & paper	Academic Registry (AR) (signed out to Academic staff as needed)	Current year plus previous five years
Student Transcripts (Academic): electronic	Academic Registry	In perpetuity
Student Additional Requirements Agreement (SARA) forms re disability: paper	Academic Registry	Life cycle of the student plus one year
Pass Lists: electronic and paper	Academic Registry	In perpetuity
Mark Schedules: electronic and paper	Academic Registry	In perpetuity.
Assessment Forms electronic and paper	Academic Registry	Current year plus previous five years
Student Academic Record: electronic & paper	Faculty & Programme offices (signed out to Academic staff as needed).	Kept until student leaves University. Upon leaving documents are sent to Academic Registry to be archived in accordance with Retention Policy for AR Student files.

Student Services

Data Source	Location	Retention Policy
Counselling notes, paper and electronic	Counselling	7 years from leaving date of subject.
Health notes, paper and electronic	Health	7 years from leaving date of subject.
Disability assessment notes, paper and electronic	Disability	6 years from leaving date of subject.
Advice notes, paper and electronic	Financial Advisor	6 years from leaving date of subject.
Advice notes, paper and electronic	Student Advisors	6 years from leaving date of subject.
Advice notes, paper and electronic, destinations data	Careers Advice	3 years from leaving date of subject.

Finance

Data Source	Location	Retention Policy
Credit card details student/parents for regular payment plans	Finance	Until payment plan has ceased.
Invoices unpaid/paid	Finance	6 years.
Student/Student Loans Company records	Finance	6 years.

Human Resources

Data Source	Location	Retention Policy
Staff Record	HR	6 years after leaving date of staff member.
Unsuccessful job applications	HR	1 year.
PDRP (Personal Development Record)	Line Managers	Returned to HR when staff member leaves.
Disciplinary Case Investigation notes	HR – separate from Staff Record	6 years after leaving date of staff member.
Sickness Records	HR	6 years after leaving date of staff member.
Criminal Records Bureau documentation	HR	6 months, in line with CRB documentation.
Accident at Work Records	HR	3 Years after the date of the last entry

Accommodation

Data Source	Location	Retention Policy
Conference/Accommodation Records	Accommodation offices across both campuses	1 year after event
Public Accommodation Records (summer B&B)	Accommodation offices across both campuses	1 year after event
Student Accommodation Records	Accommodation offices across both campuses	After student leaves and account is settled

Marketing

Data Source	Location	Retention Policy
Student Graduate information	Marketing	Award information is retained on SITS in perpetuity
Potential Student Marketing information	Marketing	As required

Academic Quality and Standards Unit

Data Source	Location	Retention Policy
Student Academic Records	Academic Quality and Standards Unit	Until case file is closed
External Examiners Personal Details	Academic Quality and Standards Unit	2 Years after last engagement
External Advisors	Academic Quality and Standards Unit	2 Years after last engagement
Research Candidates Assessors	Academic Quality and Standards Unit	2 Years after last engagement
Academic CV's on Programme Approval Documentation	Academic Quality and Standards Unit	For the life of the programme.
Mitigating Circumstances Forms	Academic Quality and Standards Unit	4 years after form submission.
Appeals Against Board of Exam	Academic Quality and Standards Unit	10 years after appeal.
Student Complaints	Academic Quality and Standards Unit	10 years after complaint.
Office of the Independent Adjudicator for Higher Education Case Notes	Academic Quality and Standards Unit	10 years after case.
Ethical Review Applications	Academic Quality and Standards Unit	Kept as long as research project is active
Research Assessment Exercise – documentation staff CV	Academic Quality and Standards Unit	Kept until the next RAE.

Appendix 4.

Data Protection Guidelines for University Staff

1. Introduction

The new Data Protection Act, which is concerned with the handling of personal information, came fully into force on 1 March 2000. The new Act is more stringent than the 1984 Act as, among other things, it covers both manual and electronic records and stipulates security standards.

2. Standard Information

Most staff process information about students on a regular basis e.g. taking registers, writing reports or references, data input to the University's central student information database (SITS), or as part of a pastoral or academic supervisory role. The University will ensure through registration procedures that all students are notified of such processing, as required by the Act, and give their consent where necessary. The information that staff deal with on a day-to-day basis is "standard" and covers categories such as:

- General personal details such as name, address and date of birth;
- Details about class attendance, course work marks and grades and associated comments;
- Notes of personal supervision, including matters about behaviour and discipline;
- Sponsorship details.

3. Sensitive Information

Information about a student's physical or mental health, ethnicity or race, political or religious views, trade union membership, sexual life, or criminal record is sensitive information under the Act. Such information can only be collected and processed as required by law, e.g., by the Children's Act 1989, or with the student's **express (written) consent**. Examples:

- Disability records
- keeping of sick notes;
- recording information about dietary needs, for religious or health reasons, prior to taking students on a field trip;
- recording information that a student is pregnant, as part of pastoral duties.

Disclosure of such information without consent is permitted only in "life or death" circumstances, e.g., if a student is unconscious, a tutor can tell medical staff that the student is pregnant or a Jehovah's Witness.

Sensitive information must be protected with a **higher level of security**. It is recommended that sensitive records are kept separately in a locked drawer or filing cabinet, or in a password-protected computer file. Where such information is taken off the main University sites, for example on a memory stick or laptop, the measures to be taken to safeguard such information should be implemented in accordance with advice from IT or the Data Protection Officer. If you (or one of your students) are holding, or intending to hold, sensitive personal information which is outside standard University processing, e.g., for a research project, you should notify the Data Protection Officer.

4. Processing of Personal Information

Processing refers to any action involving personal information, including obtaining, viewing, copying, amending, adding, deleting, extracting, storing, disclosing or destroying information. When processing personal information, you must comply with the **data protection principles**, which are set out in the Data Protection Policy. In particular, you should ensure that records are:

- accurate
- up-to-date
- fairly and legally obtained.

5. Project and Research Supervisors

If you supervise students doing work which involves the processing of personal information, you should ensure that those students are aware of the Data Protection Principles, in particular, the requirements to notify and to obtain the data subject's consent where appropriate. Students should be referred to the Data Protection Officer for further information.

6. Handling Enquiries

When students ask to see information about themselves, you should, where possible, deal with these enquiries informally. If an informal response is not appropriate, you should advise the student to make a formal **Subject Access Request** under the Data Protection Act. Such Requests should be directed to the Data Protection Officer.

You should not disclose personal information over the **telephone** unless you are able to validate the identity of the student.

You may disclose personal information to **other staff members** who require the information in order to carry out their normal duties.

You should not disclose personal information to any **third party**, e.g., to a parent or sponsor, except with the consent of the student.

In **exceptional and urgent circumstances** (e.g., cases where there are reasonable grounds for believing that an individual has become a danger to him/herself or others, or has committed / is about to commit a serious crime), you may release personal information directly to a law officer. Please contact the Data Protection Officer in such cases. Be sure to establish the identity of the law officer before releasing the information, and get an emailed or faxed copy of the request, and keep a record of the incident including name, date, circumstances and information disclosed.

7. Examination Marks

You should be aware that students are now entitled to see preliminary marks and comments, which contribute to final assessments. Committee minutes will also be subject to access requests unless they are anonymised.

Similarly, when writing an **academic reference**, you should keep in mind that it may be subject to an access request by the student to the recipient.

8. Private Files

The case for holding “private”, separate files has to be justified as being in the interest of the student (e.g., where the data is particularly sensitive) and the information contained in them will be subject to the student’s right of access. To ensure compliance with the notification requirements of the Act, you must inform the Data Protection Officer that you are holding such files. Wherever possible, you should avoid duplication or fragmentation of student files.

9. Home Working

When working from home or on a laptop, you must maintain appropriate levels of security, including virus checking. It is recommended that you work on UBS memory sticks so that personal information is not stored on your domestic PC. Special care should be taken in the transport of personal information:

- carry paper files and memory sticks in a locked briefcase;
- store briefcases and laptops in the boot of the car;
- memory sticks should be password protected.
- Emails that contain personal information must remain on University systems and not sent or received on staff’s personal (non work) email accounts.

10. Exemption for Research Records

There is an exemption under the 1998 Act for research and statistics. Information collected for the purpose of one piece of research can be used for other research, without breaching the “specified processing” principle (see the Data Protection Policy), and can be kept indefinitely. For example, staff and students involved in academic research can keep records of questionnaires and contacts, so that the research can be re-visited at a later date, or so that, in support of a research project looking at an associated area, they can re-analyse the information. Researchers must ensure that the final results of the research do not identify the individual, or they will be subject to access requests under the 1998 Act.

This exemption is only applicable to academic research and cannot be relied on to prevent access to information about a particular individual, following research carried out for a redundancy or efficiency exercise, for example.

Appendix 5

Data Protection Guidelines for Students

All students shall:

- ensure that all personal information which they provide to the University is accurate and up-to-date;
- inform the University of any changes to that information, for example, changes of address;
- check the information which the University shall make available from time to time, in written or automated form, and inform the University of any errors or, where appropriate, follow procedures for up-dating entries on computer forms. The University shall not be held responsible for errors about which it has not been informed.

Students who use the University computer facilities may, from time to time, process personal information (for example, in course work or research). In those circumstances, they must seek guidance from the Faculty, which will provide further information about this requirement. The Faculty may well refer the student to the Data Protection Officer.