



Data Protection Policy (2008)

1 Introduction

- 1.1 Canterbury Christ Church University holds and processes information about employees, students, and other data subjects for academic, administrative and commercial purposes, in accordance with the Data Protection Act 1998 ('the Act'). The Act applies to data held in manual paper files as well as on electronic systems. To comply with the Act, information must be collected and used fairly, stored safely and only disclosed lawfully to a third party.
- 1.2 When handling such information, the University, and all staff or others who process or use any personal information, must comply with the Data Protection Principles set out in the Act. In summary, these state that personal data shall be
- 1.2.1 processed fairly and lawfully
 - 1.2.2 obtained for specified and lawful purposes and not further processed in a manner incompatible with those purposes
 - 1.2.3 adequate, relevant and not excessive
 - 1.2.4 accurate and, where necessary, up to date
 - 1.2.5 kept for no longer than necessary
 - 1.2.6 processed in accordance with data subjects' rights
 - 1.2.7 protected by appropriate security
 - 1.2.8 not transferred to a country outside the European Economic Area without adequate protection
- 1.3 The University, and all staff or others who process or use any personal information, must ensure that they follow these principles at all times. To ensure this happens, the University developed this Data Protection Policy.
- 1.4 Compliance with the Act is the responsibility of all members of Canterbury Christ Church University. A breach of the Data Protection Policy, whether deliberate or through negligence, could lead to disciplinary action or withdrawal of access to University facilities. A breach of the Act might also lead to legal or regulatory proceedings. Any questions or concerns about the interpretation or operation of this policy should be taken up with the University's Data Protection Officer (see Section 4).
- 1.5 The commitment of the University is to ensure that every employee and registered student complies with the Act to ensure the confidentiality of any personal data held by the University, in whatever medium.

2 Registration

- 2.1 To comply with the Act, the University makes an entry in the Data Protection Register maintained by the Information Commissioner.
- 2.2 Details of the University's current entry in the Data Protection Register are available on the Information Commissioner's web site

(<http://www.informationcommissioner.gov.uk/eventual.aspx?id=34>). The entry can be found by selecting the option to search 'Public Register of Data Controllers'. When the search form is displayed, it is possible to locate the entry by typing 'Canterbury Christ Church University' into the Name box and then click on Search

2.3 The University notified the Information Commissioner that personal information might need processing for the following purposes:

- 2.3.1 Staff, Agent and Contractor Administration
- 2.3.2 Advertising, Marketing, Public Relations and General Advice Services
- 2.3.3 Accounts and Records
- 2.3.4 Education
- 2.3.5 Student and Staff Support Services
- 2.3.6 Research
- 2.3.7 Other Commercial Services
- 2.3.8 Publication of the University Newsletter
- 2.3.9 Crime Prevention and Prosecution of Offenders
- 2.3.10 Alumni Relations

2.4 The Register Entry provides:

- 2.4.1 an explanation of the purposes for which personal information may be used
- 2.4.2 details of the types of data subject about whom personal information may be held
- 2.4.3 details of the types of personal information that may be processed
- 2.4.4 details of the individuals and organisations that may be recipients of personal information collected by the University
- 2.4.5 information about transfers of personal data.

2.5 The University is required to ensure that its entry in the Register is correct and up to date. The Data Protection Officer must be informed immediately of new applications or purposes for which data is held that may affect the University's registration.

3 Exemption from Registration

3.1 There are a few cases where personal data may be exempt from Registration; details can be obtained from the Data Protection Officer. Among the more significant exemptions are data kept by individuals purely for private domestic purposes and files comprising simply names and addressing information. Any members of the University who hold files that they consider may be exempt from Registration must consult with the Data Protection Officer.

3.2 In some cases, however, registration should not be done through the University. This would be the case if the data could not be regarded as being under the control of the University. For example:

- 3.2.1 editorial material or records for journals, or membership records of learned societies, which should be registered by the learned society or other body, or by the individual
- 3.2.2 data relating to consultancy work, which should be registered by the client
- 3.2.3 data, which is held in relation to the care of patients, which should be registered by the NHS Trust concerned. However, if such data is also used by members of staff undertaking research as members of the University, there is a need to register this use of data.

3.3 The University is registered as a computer bureau as well as a data user, allowing it to perform data processing on behalf of external organisations.

4 Managerial Responsibility for Data Protection

- 4.1 The University Data Protection Officer is the named contact with the Information Commissioner. The University Data Protection Officer ensures that the University Data Protection Registration is kept up to date based on information received from the Heads of Department. The Data Protection Officer provides advice to the University and its members on data protection issues.
- 4.2 The University Data Protection Officer is Robert Melville, Assistant University Secretary (e-mail foi@canterbury.ac.uk).
- 4.3 The University is the Data Controller under the Act. The Governing Body is ultimately responsible for ensuring compliance.
- 4.4 Heads of Department have day-to-day responsibility for ensuring compliance with the Act. They are responsible for ensuring that the personal data held by their department is kept securely and used properly, within the terms of the Act. They are also responsible for informing the Data Protection Officer of the types of personal data held in their department, and any changes or new holdings.

5 *Notification of Data Held and Processed*

- 5.1 All staff, students, and other users are entitled to:
- 5.1.1 know what personal information the University holds and processes about them and why
 - 5.1.2 know how to gain access to it
 - 5.1.3 know how to keep it up to date
 - 5.1.4 know what the University is doing to comply with its obligations under the Act
- 5.2 Information about the types of personal information held about students by the University will be outlined in the Student Handbook and queries can be addressed to the Director of Student Services. Queries about personal information held about staff should be addressed to the Personnel Department.

6 *Staff Guidelines for Data Protection*

- 6.1 All members of staff are responsible for:
- 6.1.1 checking that any information that they provide in connection with their employment is accurate and up to date
 - 6.1.2 informing the University of any changes to information they provided, for instance changes of address and qualifications
 - 6.1.3 checking the information the University makes available from time to time, in written or automated form
 - 6.1.4 informing the University of any errors or, where appropriate, follow procedures for up-dating entries
- 6.2 The University is not responsible for errors about which it has not been informed.
- 6.3 All members of staff should ensure that any data in their possession or control complies with the University's Data Protection Registration. That includes data for such purposes as assessment, research, and personnel functions.
- 6.4 A member of staff who supervises students undertaking work that entails processing personal information must ensure the students are aware of the Data Protection Principles, in particular, the requirement to obtain the data subject's consent where appropriate (see Section 1).

- 6.5 The Head of Department should be consulted if a member of staff has any doubts about personal data that the member of staff controls. Alternatively, advice may be sought from the University Data Protection Officer.
- 6.6 Personal names and e-mail addresses of University members will normally be published on the World Wide Web. Individuals may however indicate to the Data Protection Officer that they do not wish their personal details to be disseminated in this way. Those responsible for producing pages for the World Wide Web Facility, whether for general University information or for specific departments, are responsible for ensuring that any individual named on that page has not refused permission to publish their name and e-mail address, by checking either with the individual or with the Data Protection Officer.

7 Data Security

- 7.1 All members of staff are responsible for ensuring that:
- 7.1.1 any personal data that they hold, whether in Electronic or Paper format, is kept securely
 - 7.1.2 personal information is not disclosed either orally or in writing, accidentally or otherwise, to any unauthorised third party
- 7.2 Unauthorised disclosure may be a disciplinary matter, which is addressed under the University Disciplinary Procedures.
- 7.3 On incoming and internal mail, only the addressee (or a person such as a secretary acting on the *specific* instruction of the addressee) should open items marked "Personal" or "Private and Confidential", or which appear to be of a personal nature. Unless mail items are marked in this way, they will be considered not to contain confidential information. Members of staff are discouraged from using their University address for non-University matters.
- 7.4 Each Head of Department is responsible for ensuring appropriate technical and organisational measures are taken within the department to ensure against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, such data. The Head of Department is responsible for keeping the Data Protection Officer informed of changes in the collection, use, and security of personal data within their department.
- 7.5 All members of staff and students dealing with data should ensure that casual access to data is not possible, for example by members of the general public seeing VDU screens or printouts. VDU screens should be cleared after use, and terminals should not be left unattended without being logged off. Printouts should be kept securely, and shredded when no longer required. Particular care must be taken when laptop computers are used in public places or on public transport, and when working at home.
- 7.6 All members of staff and students dealing with data should hold appropriate back up or duplicate copies of data, in case of unauthorised destruction or loss of data.
- 7.7 It should not be assumed that documents sent by Electronic Mail are secure. Confidential information should not be sent by e-mail, or where it must be, it should be encrypted before transmission. It is not advisable to send sensitive data by e-mail.
- 7.8 While the University will normally endeavour to honour the privacy of personal electronic mail, the University will normally be the legal owner and may inspect it, for example to ensure the security of systems by virus checking. In addition, the University may be required to disclose it as part of a Data Protection Act disclosure or other civil or criminal legal process.

8 Student obligations

- 8.1 Students must
- 8.1.1 ensure that all personal data provided to the University is accurate and up to date
 - 8.1.2 inform the University of any changes to that information, for example, changes of address
 - 8.1.3 check the information that the University makes available from time to time, in written or automated form
 - 8.1.4 inform the University of any errors or, where appropriate, follow procedures for up-dating entries
- 8.2 The University shall not be held responsible for errors of which it has not been informed.
- 8.3 Students who use University computer facilities may process personal data, for example in course work or dissertations, only with the explicit consent of the Programme Director or Head of Department.
- 8.4 Students undertaking research projects using personal data must ensure that:
- 8.4.1 the research subject is informed of the nature of the research and consents to their personal information being used
 - 8.4.2 their supervisor is informed of the proposed research before it begins, and ensures that the University is licensed to undertake this kind of research
 - 8.4.3 all information is kept securely

9 *Subject Consent to Processing Sensitive Information*

- 9.1 In many cases, the University can only process personal data with the consent of the individual. In some cases, if the data is sensitive, there is a requirement to obtain express consent in advance. 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 a member of staff.
- 9.2 Some jobs or programmes bring individuals into contact with children, including young people under the age of 18 years. The University has a duty to ensure that members of staff are suitable for the job and students for the programmes offered.
- 9.3 The University also has a duty of care to all staff and students and must therefore make sure that employees, and those who use University facilities, do not pose a threat or danger to other users.
- 9.4 The University may ask for information about a person's health, particular health needs, such as allergies to particular forms of medication, or any conditions such as asthma or diabetes, for use in the event of a medical emergency.
- 9.5 The University may also ask for information about a person's criminal convictions, race, disability, gender and family details. This is to ensure the University is a safe place for everyone, or to operate other policies such as the sick pay policy or equal opportunities policy.
- 9.6 Where the information is considered sensitive, prospective staff and students should be asked to give signed Consent to Process regarding particular types of information when an offer of employment or a place on a programme is made.

10 *Publication of University Information*

- 10.1 The University publishes information in accordance with the requirements of the Freedom of Information Act 2000. The University maintains a Publication Scheme that sets out the information published under the various classes.

- 10.2 Internal phone lists will not be published documents under the Publication Scheme, but may still enter the public domain.
- 10.3 Any member of staff having good reason for wishing personal details in these lists or categories to remain confidential should contact the University Data Protection Officer. Similarly, any student having good reason for wishing details in these lists or categories to remain confidential should contact the University Data Protection Officer.

11 *Special Cases*

Examination Marks:

- 11.1 The Act recognises examination marks as a special case, and provides for the special treatment of these. Requests from students about confidential examination results held on computer should be treated as subject access requests, and should be referred to the Data Protection Officer in the first instance.

Video Recordings:

- 11.2 The Act applies to data held on video recorders that is obtained from closed circuit television surveillance systems.

12 *Rights to access information*

- 12.1 Staff, students, and other users of the University facilities have the right to access any personal data that is being kept about them in a relevant filing system. Any person who wishes to exercise this right should make their request in writing to the Data Protection Officer. The fee of £10, which is the statutory charge, must accompany the application. The Data Protection Officer may require the following from the individual:
- 12.1.1 evidence of their identity
 - 12.1.2 an indication of the type of information sought and/or where they believe this information is held
- 12.2 The University aims to comply with requests for access to personal information as quickly as possible, but will ensure that it is provided within 40 days unless there is a good reason for delay. In such cases, the reason for delay will be explained in writing to the data subject making the request.

13 *Retention of Data*

- 13.1 The University retains certain information in line with financial, legal, or archival requirements. Queries on retention times should be addressed to the Data Protection Officer.

14 *Research Purposes Exemption*

- 14.1 Data collected fairly and lawfully for the purpose of one piece of research can be used for other research, providing that the results of the research do not identify the individual. Such data must not be processed to support measures or decisions with direct consequences for the individuals concerned, or in a way that is likely to cause substantial damage or distress to any data subject. Records of questionnaires and contacts may be kept in order that the data can be revisited or reanalysed. This exemption is only applicable to academic research, and cannot be used to provide information about a particular individual.

Document control/change history				
Version	Author(s)	Date	Circulation	Comments
2.1	RM	29 March 2005	CCCUC	Approved by Information Services Committee and Senior Management Team
2.2	RM	27 July 2005		Changes reflecting University status
2.3	RM	September 2008		Reformat only by IE to match other Info Sec Policies

Document approval and review	
Approved by:	Information Systems Committee
Date approved:	
Review date:	
Author(s):	Assistant University Secretary
Owning Department:	University Solicitor