Policy on the Retention of Student Data and Records

1. Purpose

1.1 This policy defines the principles, time periods, mechanisms and responsibilities for the university's retention of student personal data. The university Retention Schedule sets out the agreed timeframe for the retention of all student personal data and records.

2. Definition and scope of student personal data and records

2.1 'Student' in the context of this policy is defined as:

2.1.1 any individual who has ever reserved or registered on a programme or module of taught study or applied for a research higher degree with the university

2.1.2 members of the public requesting materials that require a Personal Identifier

2.1.3 students on collaborative and partnership schemes registered as Open University (OU) students

2.1.4 individuals registered for bespoke offerings through the Centre for Professional Learning and Development (CPLD)

2.1.5 students of other institutions with qualifications validated by the Open University or students of awarding bodies where the University acts as the guardian of that awarding body's archive (eg: CNAA Council for National Academic Awards).

2.2 As a student may continue to study throughout their life, certain records will be kept for 120 years from date of birth to cover this eventuality. In general, most records relating to the student relationship will be deleted after 6 years from completing an individual module. Certain records relating to practice based learning or research qualifications will be retained for 6 years after completion/ termination of qualification. See the retention schedule for further details and exceptions.

2.3 Specifically excluded from this policy are:

2.3.1 members of the public who contact the university for any other reason including those purchasing products through the Open University Worldwide (OUW)

2.3.2 members of the public who self register for access to on-line services and participate in forums where it is not necessary to be a student

2.3.3 alumni data: Personal details transferred to Alumni Office systems on student qualification. (However, an alumnus may also be considered a current student if they register for modules subsequent to qualification.)

2.4 This policy covers all student data, information, records and content relating to university business which has been created by university staff or student (eg: in on- line forums) and:

2.4.1 relates to an identifiable individual (eg: identified by name, PI and/or contact details)

2.4.2 is kept in any medium or format (eg: text, sound, image, paper, electronic, document or database)

2.5 Generally, student records will relate to the management of the relationship between the OU and its students, for example:

2.5.1 contractual records documenting admission and enrolment, payment of tuition fees, disciplinary proceedings

2.5.2 transcript records documenting the modules and qualifications undertaken, academic progress, etc

2.5.3 student support records, documenting contact and use of services such as disability support, careers services, study skills support, counseling, Library etc.[1]

3. Legislative and regulatory framework

3.1 The Data Protection Act 1998 requires that student records should only be retained for as long as is necessary. JISC[2] guidance suggests that necessary activities include being able to:

3.1.1 fulfil and discharge the contractual obligations established between the institution and the student, including the completion of any non-academic disciplinary action

3.1.2 provide information on the academic career and achievements of the student to employers, licensing/regulatory bodies and other organisations, as well as to the student as part of their lifelong learning record

3.1.3 record the activities of the student as an individual and as a consumer of student support and other institutional services as a means of managing those services and planning and developing them in the future.[3]

3.2 The Data Protection Act 1998 also requires that personal data should be accurate and up-to-date. As a student can continue to study modules for many years, the deletion of certain information after a set time with the requirement for the student to re-submit up-to-date information would ensure compliance with this principle, eg: information on a student's disability.

3.3 The contractual relationship between the institution and the student is subject to the same statutory limitations on action as any other contract, and therefore the Limitation Act 1980 and Prescription & Limitation (Scotland) Act 1973 apply to the student

---

1 JISC Infonet, January 2007, 'HEI Records management: Guidance on Managing Student Records' page 4 http://www.jiscinfonet.ac.uk/partnerships/records-retention-he/managing-student-records

2 JISC: Joint Information Systems Committee (www.jisc.ac.uk)

3 JISC Infonet, January 2007, 'HEI Records management: Guidance on Managing Student Records' pages 6-7 http://www.jiscinfonet.ac.uk/partnerships/records-retention-he/managing-student-records

relationship with the OU. I.e. generally, legal action brought by either a student or the University must commence within six years of the alleged breach of contract.

3.4 Regulators, eg: HEFCE, require us to keep information for certain periods of time.

3.5 Student data may be affected by other legislation relating to particular areas of activity.

4. Principles for the management and retention of personal data

4.1 The timeframe for retaining personal data must be in line with legislative and regulatory requirements (see section 3) and must meet business requirements. However, the choice of retention timeframes should be kept to a minimum in order to simplify the task of managing large stores of data.

4.2 Long term records (life of student -120 years from date of birth/permanent)

4.2.1 There is an expectation by students, employers and Government agencies and members of the public that Universities should retain a permanent core record of student names, the modules and qualifications studied and their outcomes.

4.2.2 In addition to 4.2.1 there are records and data which need to be retained whilst a student might continue to study with the OU. These will be retained for the 'life of student' (which is taken to be 120 years from date of birth).

4.2.3 Data required for management, development and research may be retained outside the student records systems for the long term. In storing this data, the name and address of a student will be removed and, in line with the Data Protection Act 1998, the data will not be used to support any actions or decisions that affect or cause distress or damage to the individual. The exception will be research data which with student agreement requires follow-up contact.

4.3 Legal, contractual and regulatory requirements

In line with section 3.3, there is a legal/contractual requirement to keep records and data relating to fee payment, registration, etc for six years after the student has completed or withdrawn from the module or programme.

4.4 Student support services (6 years from completion of transaction)

There are cases where it is necessary to keep records of student support for 6 years to inform ongoing contact with students. This includes careers support, disability support, study issues advice, research student support, and course choice.

4.5 Operational records (up to 3 years from completion of activity)

Data relating to the student as a user of student support services or day to day administration eg: tutor allocation, graduation ceremonies, residential school requirements, and enquirers. Where these records are kept on a central electronic system they will be retained for 3 years.

4.6 Accuracy of records

As stated in section 3 above, personal data must be accurate. As a student can continue to study modules for many years, the deletion of certain information after a set time with the requirement for the student to re-submit up-to-date information would ensure compliance with this principle, eg: information on a student's disability.

4.7 Sharing data with third parties

4.7.1 Personal data owned by the university may, on occasion, be shared with third parties; and conversely personal data owned by other organisations may be shared with the OU. Where the third party is acting as our agent on the basis of university instructions (eg: outsourced corporate or student services, projects involving consultants, outsourced technology solutions, market research etc), the university remains the data controller. The third party must be contracted to adhere to the university's student data retention and security policies, as well as the UK Data Protection Act or equivalent legislation'. In relation to projects which use personal data to inform institutional research, eg: those undertaken by market research agencies, the contract would usually require them to destroy data immediately after project completion. For other types of research projects which may use personal data (e.g. third party funded, RCUK funded, doctoral research), the management and archiving of data must be in accordance with university and funder guidelines as well as with the Data Protection Act 1998 or equivalent legislation.

4.7.2 Where professional bodies and partner organisations require the university to retain student data and records for significant periods of time the periods will be clearly specified in the agreements between these organisations and the OU and then added to the Retention Schedule (see paragraph 7.3 below).

4.7.3 Where the third party is taking ownership of OU student data (eg: HESA, sponsors, OUW and their partners, professional bodies etc) the third party becomes the data controller. The data is then subject to that third party's data retention policies. Where a third party is sharing their student details with the OU or OUW, then the OU and OUW must still hold that data in compliance with the UK Data Protection Act. See the university's Data Protection policy.

4.7.4 Third parties with a regulatory or statutory remit may require information from the OU without stating a limit for the age of data that may be requested. In these cases, a retention period should be set on a basis of risk analysis. For example, The Office of the Independent Adjudicator for Higher Education may require data of any age from the OU to support the investigation of complaints and appeals.

4.8 Due to the constraints of some of the databases and repositories containing student data, other pragmatic events or time periods may be used to ensure that the destruction of data occurs within a reasonable time of the retention period stated for the data/activity type. For example, DIP records will need to be deleted within a fixed period from the date they have been scanned. Where the Retention Schedule requires that a DIP record is kept for a specific timeframe from module completion it will be necessary to include a calculation for the maximum amount of time it may take for completion ie: 5 years from date scanned.

4.9 It is good information management practice to destroy information when it becomes redundant. This ensures that retrieving current information is more efficient, and that redundant information is not retrieved in error because it still exists. Student data retention periods should be set taking JISC recommendations of good practice into account, as well as legal and regulatory requirements.

4.10 The retention periods for student data and records are incorporated in the university Retention Schedule.

5. Roles and responsibilities

5.1 The University Secretary is the Information Owner for the university.

5.2 The Director, Students is the university officer responsible for student data and records within the university.

5.3 The Records Manager provides tools, advice and guidance to ensure that university records are maintained according to legislation and best practice.

5.4 It is the responsibility of each Head of Unit to ensure that there are local policies and procedures in place for the regular destruction of data and records held in local systems according to the university Retention Schedule.

5.5 It is the responsibility of Associate Lecturers to ensure that they comply with this policy in relation to student data and records held on private systems, e.g. personal email accounts, personal computers or hardware.

5.6 It is the responsibility of students using personal data and information accessible within the university's on-line learning systems to handle such data in line with the Computing Code of Conduct.

5.7 Student data and records in central databases and record systems, currently CIRCE, VOICE, DIP and on-line learning systems will be destroyed centrally in line with this policy and the university's Retention Schedule.

6. Maintenance of policy

6.1 The Policy, and compliance with the policy, will be reviewed every 3 years at the instigation of the Director, Students. There will be an annual review to ascertain if amendments to the Retention Schedule or policy are required due to changing legislation or business requirements.

6.2 The Director, Students (or nominee) may at any time request individual stakeholders to submit a report on their compliance with this policy.

6.3 The Retention Schedule is updated on a rolling basis by the Records Manager, aiming to review all entries within 5 years of the last update. Each amended entry relating to student data will be approved by the Director, Students, or his/her nominee.

6.4 Revisions to the Retention Schedule or queries in interpreting this policy should be directed in the first instance to the Records Manager. Issues relating to legal non-compliance must be forwarded to Senior Manager, Information Compliance.

6.5 All student data and records require a robust business reason for them to be kept. If a business reason for the retention of student data cannot be articulated, then it should be destroyed. The case must include evidence of the frequency with which this data is referred to over time; and an analysis of the financial or other risk of not being able to refer to the data.

7. Related policies

- Data protection policy
  www.open.ac.uk/students/charter/essential-documents/a-to-z/#n287
- Freedom of information code of practice
  www.open.ac.uk/students/charter/essential-documents/a-to-z/#n289