Study Group UK & Europe

Policy on the Retention of Student Data & Records

StudyGroup

studygroup.com

Contents

1. Purpose

1.1 This policy defines the principles, time periods, mechanisms and responsibilities for the institutions' retention of student personal data. The Retention Schedule sets out the agreed timeframe for the retention of all student personal data and records, updated in 2018 to meet GDPR requirements.

2. Definition and scope of student personal data and records

2.1 'Student' in the context of this policy is defined as any individual who has ever 'reserved' a place or registered on a programme.

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 7 years from completing an individual module. See the Retention Schedule (Appendix 1) for further details and exceptions.

2.3 Specifically excluded from this policy are members of the public who contact the Institution for any other reason.

2.4 This policy covers all student data, information, records and content relating to the Institution's business which has been created by Institution staff or students (e.g.: in online forums) and:

2.4.1 relates to an identifiable individual (e.g.: identified by name, PI and/or contact details)
2.4.2 is kept in any medium or format (e.g.: text, sound, image, paper, electronic, document or database)

2.5 Generally, student records will relate to the management of the relationship between the Institution 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, counselling, Library.

3. Legislative and regulatory framework

3.1 The General Data Protection Regulation (GDPR) is a European-wide law, and the Data Protection Act 2018 is the UK's implementation of the General Data Protection Regulation (GDPR). It places greater obligations on how organisations handle personal data. It came into effect on 25 May 2018.

The GDPR applies to 'personal data', which means any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier. The GDPR applies to processing carried out by organisations operating within the EU. It also applies to organisations outside the EU that offer goods or services to individuals in the EU.

Source: Information Commissioner's Office: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/

The Joint Information Systems Committee (JISC) guidance for the HE sector 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 Institution services as a means of managing those services and planning and developing them in the future.

3.2. GDPR 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, e.g.: 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 relationship with the Institution. i.e. generally, legal action brought by either a student or the Institution's must commence within six years of the alleged breach of contract.

3.4 Regulators 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 (120 years from date of student birth/permanent)

4.2.1 There is an expectation by students, employers and Government agencies and members of the public that educational institutions 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 Institution or a University they progress to. 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 GDPR, 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 seven 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 4 years from completion of activity)
If applicable, data relating to the student as a user of student support services or day to day administration e.g.: tutor allocation, graduation ceremonies, residential school requirements, and enquirers. Where these records are kept on a central electronic system, they will be retained for up to 4 years (see Appendix 1, Retention Schedule).

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, e.g. information on a student's disability.

4.7 Sharing data with third parties

4.7.1 Personal data owned by the Institution may, on occasion, be shared with third parties; and conversely personal data owned by other organisations may be shared with the Institution. Where the third party is acting as our agent on the basis of

Institution's instructions (e.g. outsourced corporate or student services, projects involving consultants, outsourced technology solutions, market research etc.), the Institution remains the data controller. The third party must be contracted to adhere to the Institution's student data retention and security policies, as well as the GDPR or equivalent legislation. In relation to projects which use personal data to inform institutional research, e.g.: 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 that may use personal data (e.g. third-party funded), the management and archiving of data must be in accordance with the Institution's and funder guidelines as well as with the GDPR or equivalent legislation.

4.7.2 Where professional bodies and partner organisations require the Institution 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 Institution and then added to the Retention Schedule (see paragraph 7.3 below).

4.7.3 Where the third party is taking ownership of Institution student data (e.g.: University partners), 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 Institution, then the Institution must still hold that data in compliance with the GDPR.

4.7.4 Third parties with a regulatory or statutory remit may require information from the Institution 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 (OIA) may require data of any age from the Institution 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, SID records will need to be deleted within a fixed period from the date they have been scanned. Where the Retention Schedule requires that a SID 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 i.e.: 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 Institution's Retention Schedule.

5. Roles and responsibilities

5.1 The Head of Centre or Principal is the Information Owner for the Institution at ISC, IC and College.

5.2 It is the responsibility of each Head of Centre 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 Institution's Retention Schedule.

5.3 It is the responsibility of staff 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.

5.4 It is the responsibility of students using personal data and information accessible within the Institution's on-line learning systems to handle such data in line with any applicable code of conduct.

5.5 Student data and records in central databases and record systems and on-line learning systems will be destroyed centrally in line with this policy and the Institution's Retention Schedule.

6. Maintenance of policy

6.1 The Policy, and compliance with the policy, will be reviewed every three years at the instigation of the Academic Registrar. There will be an annual review in consultation with the Director, Risk and Compliance and GDPR colleagues to ascertain if amendments to the Retention Schedule or policy are required due to changing legislation or business requirements.

6.2 The Director, Risk and Compliance (or nominee) or the Academic Registrar (or nominee) may at any time request individual stakeholders to submit a report on their compliance with this policy.

6.3 Each amended entry relating to student data will be approved by the Director, Risk and Compliance or nominee or Academic Registrar or nominee.

6.4 Revisions to the Retention Schedule or queries in interpreting this policy should be directed in the first instance to the Academic Registrar. Issues relating to legal non-compliance must be forwarded to Director, Risk and 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, 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

General Data Protection Regulation (2018) : https://my.studygroup.com/Pages/GDPR.aspx

Appendix 1

Retention Schedule

This schedule sets out retention periods for a range of records relating to ISC/IC and Bellerbys College student and programme administration. It aims to ensure that these records are managed consistently across the network and are retained for as long as necessary to meet operational and business needs, and to demonstrate compliance with legal and regulatory requirements.

It applies to all the listed categories in whatever format they are held (i.e. paper or electronic). The retention periods take into account recommendations of the JISC HE Retention Schedule and common practice across the UK higher education sector. Unless otherwise agreed, it is the responsibility of Heads of Centre to retain the items listed in this document.

Document Version Control

Document Source		Academic Office	
Authorised to Approve		AQAEC	
Version	**Date approved**	**Update by**	**Details**
1	2015	N/A	N/A
2	February 2019	Adam Roberts, Academic Registrar	• Updated to reflect the General Data Protection Regulation (2018) and revised Retention Schedule • Version Control Document inserted.