A03 Student Record Management and Data Processing Policy

Table of Contents

1 Introduction

1.1 Purpose

SAE recognises the right to privacy of all student information and communications. As an organisation, SAE Institute is committed to complying with the provisions of relevant data protection legislation in the locations of each campus, and internationally with the General Data Protection Regulation (GDPR).

This policy describes a framework for the creation, management, and retention of student data and records within SAE Institute, recognising their purpose as essential evidence of student activity, while acknowledging the need for information privacy.

1.2 Context

This policy addresses specifics of managing student records and related data, while ensuring alignment with University partners' practices, and compliance with relevant regulation including the General Data Protection Regulation (GDPR).

1.3 Related Policies and Documents

This policy should be read in conjunction with:

- A02 Public Information Policy
- A05 Academic Quality Assurance Policy
- A14 Complaints Policy
- EU General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679)

1.4 Definitions

The following terms, used throughout this policy, are defined as:

Personal Data: defined by the GDPR as any information relating to a data subject (that is, a living, identifiable individual) and which can be held in a form in which it can be, or is being, processed automatically, either on computer systems or structured manual filing systems.

Data Subject: the identified or identifiable person to whom personal data relates.

Data Processing: covers any activity involving personal data.

Student Records: all data and physical documents relating to a student, which may contain personal data, application data, data relating to academic progress, assessment, engagement or feedback, and any other activity in which the student is involved during the course of their studies.

Record Management: addresses systematic and efficient control of the life cycle of records; that is, the period of time that records are in the custody of the organisation. The life cycle usually consists of creation or receipt; maintenance and use; and disposition.

2 Scope

This policy applies to all SAE campus involved in the delivery of validated programmes, applicants to study on these programmes, and any current or past students enrolled to those programmes.

Records of SAE processes or activities not directly involving students are managed separately, following internal SAE policies.

3 Policy

3.1 Data Collection

Student data shall only be collected with consent from the student. Explicit consent will be sought for collection of any “special categories” of personal data as defined in the GDPR.

SAE will only collect personal information from students where that information is necessary to carry out legitimate activities (such as legal compliance with regulatory bodies, or for the purposes of alumni communications). SAE will take reasonable steps to inform students of the purpose of the information collection. Data collection notices for regulatory compliance will be periodically published through the SAE website as required.

3.2 Data Processing

SAE Institute shall only use or disclose student data for the primary purpose (that is, the original stated reason) for which it was collected. Information shall not be used or disclosed for secondary purposes unless the individual has consented to such use or disclosure, or where required by law.

3.2.1 Data Quality

SAE Institute shall take all reasonable steps to ensure that personal information is accurate, complete and up-to-date at the time of collection, and will ensure to the best of its ability that any personal information collected is not misleading.

3.2.2 Data Storage

Digital student records are stored on a number of systems, including:

- proprietary or third-party Student Record Systems (SRS)
- third-party Learning Management Systems (LMS), primarily but not limited to Moodle and Canvas
- third-party cloud service providers, primarily but not limited to Microsoft and Google
- secure internal networked drive systems.

SAE aims to store all records in digital form where possible, following internal guidelines on correct naming conventions and file structures. SAE Institute shall take all reasonable steps to ensure that personal information is suitably and securely stored, including ensuring that appropriate filing procedures are in place. The security of physical file storage, digital storage, and communications will be maintained at all times. Where physical records do exist, these are stored securely in locked storage units and rooms, accessible only by authorised staff.

Processes for collecting, storing, using, maintaining, transferring and disposition of data are administered locally, and vary for different types of data. SAE follows a 'continuous improvement' approach to record management.

SAE Institute shall ensure that personal information is safe from misuse, loss, and unauthorized access, loss, or disclosure. Personal information shall be destroyed or de-identified following the appropriate review period (please refer to Appendix A), subject to legal or regulatory requirements for data retention beyond that period.

3.2.3 Security of Data

Security of records is essential to minimize risk and protect the rights of individuals about whom information is held. Senior management within each region and campus will be responsible for the safe keeping of all records, and will control the numbers of staff holding, processing and accessing student records.

Good practice should be followed, including:

- Clarity of staff authority to access, edit, or dispose of information.
- Digital records should be held on centralised systems, not individual or inaccessible locations.
- Access to confidential information should be controlled through personalized logins, password protection, and read-only settings.
- Staff should not leave computers or physical records unlocked when unattended.

Any sharing of student record information with external bodies, including regulatory authorities and University partners, should only be done by authorised staff and in line with written procedures. Such information must only be shared through secure portals (where available) or through password-protected documentation, with passwords communicated separately.

3.2.4 Data Breaches

In the event of an actual or suspected data breach, which includes all information regardless of storage media and/or type, the Procedure for Reporting and Management of Data Breaches will be followed.

3.2.5 Data Sharing with University Partners

Data sharing agreements are in place between SAE and University partner to facilitate the sharing of students' data. Processes for the secure transfer of data between institutions, including across national borders, are in place and under continual review and improvement by SAE and University staff.

Data shared with University partners will then be subject to the University policies on data processing and protection.

3.3 Disposition of Records

Student records reaching the end of their retention period will be reviewed and at this stage either (i) retained for a further period with good reason, or (ii) destroyed.

When records are destroyed, proper procedures should be put in place to ensure that they are disposed of correctly and that there is an audit trail of this destruction. Destruction of records, including any duplicates, should be authorised by the designated officer (see Appendix A). Sensitive and personal information should be destroyed in a confidential manner.

Permanent records will be held in a secure server and backed up regularly.

3.4 Responsibilities

Managers and staff at all levels of SAE are responsible for the implementation of this policy and related procedures concerning the correct input, maintenance, storage and security of student record data, in line with the duties and responsibilities of their roles. Responsibilities for specific items are listed in Appendix A. Key staff with primary responsibilities include:

- Deans
- Directorate of Academic and Student Services (DASS) staff (including Learning Managers and Quality Managers)
- Academic Coordinators
- Executive Leadership Teams (including Campus Managers, Recruitment Managers, and Finance Managers).

3.5 Retention of Student Work and Assessment

3.5.1 Assessments

A default minimum retention period of one year applies to graded assessments of student projects and assignments for all modules. In some campuses, local regulation requires a minimum retention period of three years or more; all campuses must adhere to their local procedures, and will retain student works wherever necessary to meet regulatory requirements.

This period begins from the date of the Assessment Board of the module for which the work was assessed. Original copies of works are always to be returned to the student unless it has been agreed that the work will be kept for the purposes of using as an example.

3.5.2 Use of student projects or assignments for teaching purposes

SAE Institute may retain students' work (that is, any projects or assignments submitted for assessment) for use in specific learning and teaching contexts, such as exemplars of work for future instances of a given module. This allows for:

- Student work to be used for learning and teaching purposes at any SAE campus running the programme for which the work was submitted.
- Student work to be referred to by all active students.
- Student work to be available for use from the time of the final confirmation of the grades for the module in which the project was created.

Wherever practicable, efforts should be made to anonymise personal data of the creator of the work, and that of any third parties, contained within a student work that is being used for learning and teaching purposes. Specific attention must be paid to "special categories of personal data", and in the following cases:

- visible evaluation of the assignment
- autobiographical studies such as Curricula Vitae
- use of student projects or assignments as "negative examples".

3.6 Freedom of Information

SAE fully adheres to the obligations imposed by local Freedom of Information Acts applicable to all campuses delivering validated programmes. For further information, please refer to local guidance on these obligations.

3.6.1 Data Subject Access

Students in the EU, EEA or Serbia, as Data Subjects, have the right to:

- Access and review all personal data held about them by SAE.
- Rectify or correct any inaccurate personal information held about them by SAE.
- Request a copy of the data they supplied to SAE, in a machine-readable format, or for the transfer of this data to another company.
- Request the restriction of processing of their personal data.
- Object to SAE processing their personal data.
- Request the erasure of their data (right to be forgotten).

4 Further Information

For further information on how student data is collected and processed, or on your rights, please contact your local Campus Manager.

5 Policy History

Policy Created:	June 2022
Date of Last Revision:	November 2022
Approved by:	CM, November 2022

Appendix A Retention Schedule

This schedule is not an exhaustive list and may be updated from time to time, or in line with local regulation and legislation.

	Record Type	Minimum period for which the Record Type is to be retained	Officer responsible for archiving, document retention and for maintaining the University's official record
1	Discontinued applications	A minimum of eighteen (18) months and a maximum of two (2) years from the date of the application to the University	Admissions Manager
2	Unsuccessful applications	Six (6) months after the census date of the period targeted for enrolment	Admissions Manager
3	Successful admissions information (including offer letters, applications, supporting documentation)	Seven (7) years after the student has completed/withdrawn	Admissions Manager
4	Student fees and loans information	Five (5) years after the student has completed/withdrawn	Campus Manager
5	Students' personal files. (May include personal data, details of study, admission information, awards.)	Twelve (12) years after the student has completed/withdrawn	Directorate of Academic and Student Services
6	Academic Misconduct records	Twelve (12) years after the student has completed/withdrawn	Directorate of Academic and Student Services

7	Complaints and associated information/evidence	Twelve (12) months from the completion of procedures. Note of the complaints procedure will be kept permanently.	
8	Academic achievement and qualification information (Assessment and module grades, Transcripts)	Permanent	Directorate of Academic and Student Services
9	Assessment Boards (Module, Programme, Regional, Finalist) minutes and Board reports	Permanent	Directorate of Academic and Student Services
10	Conferment lists	Permanent	Directorate of Academic and Student Services
11	Student projects (Undergraduate & Postgraduate)	Original copies to be returned to the student, unless it has been agreed that a project should be held by a local campus as an example.	Academic Coordinator
12	Other assessed work contributing to module grades	Twelve (12) months after the relevant Assessment Board meeting. Work may be held for longer may be retained longer where there is a regulatory requirement to doso.	Academic Coordinator
13	Requests for extension or deferral of assessment deadlines	Until the student has completed/withdrawn	Academic Coordinator
14	Student Representative reports	Two (2) years after the meeting for which the report was submitted	Academic Coordinator

15	Module Feedback Questionnaires	Two (2) years after submission	Directorate of Academic and Student Services
16	National Student Survey (NSS) documents	Current year plus six (6) years	Directorate of Academic and Student Services
17	Information relating to academic scholarships, awards, bursaries, and prizes	Records to be kept for five (5) years after the student has completed/withdrawn List of awards made to be kept permanently.	Directorate of Academic and Student Services
18	Timetables	Twelve (12) months after the completion of the teaching period	Academic Coordinator
19	Recordings (audio and/or visual) of teaching sessions	Twelve (12) months from the completion of the module Please refer to Recording of Learning, Teaching and Assessment Policy	Learning and Teaching Manager
20	Resources used in course delivery	Two (2) years from the completion of the module	Learning and Teaching Manager
21	Learning contracts, student formative assessments, other student-authored in-class materials	Twelve (12) months from completion of the module	Academic Coordinator
22	Ethical approval processes relating to student projects	Seven (7) years from the completion of the project	Directorate of Academic and Student Services