



REGULATIONS / POLICY LIBRARY

Privacy and Student Records Framework

DIG-001 | Digital Services

VERSION 1.0 · 18 OCTOBER 2026

INSTITUTIONAL REGULATIONS & POLICIES | IEU

Privacy and Student Records Framework

DOCUMENT CONTROL / DIG-001

Document ID	DIG-001
Document family	Digital Services
Document custodian	Data Protection / Records Owner
Version	1.0
Edition date	18 October 2026
Review cycle	Annually and following material change

1 Purpose and applicability

Applies to personal information collected through IEU forms, learning services and administration. The provisions govern the activities within the defined IEU service scope; applicable programme-specific contracts and verified rules of a separate awarding institution govern award requirements wherever relevant.

2 Policy requirements

- 01 Data is collected for specified, documented purposes with appropriate notice and legal basis.
- 02 Only the minimum necessary personal information should be requested.
- 03 Personal records are accessible only to authorized roles and approved processors.
- 04 Data sharing with awarding institutions or service vendors must be disclosed and appropriately governed.
- 05 Requests for access, correction and other applicable rights are recorded and handled under relevant law.
- 06 Retention, international transfers and breach actions require a documented operational schedule and accurate public privacy notice.

3 Operational procedure

Trigger: Personal data collection, transfer, retention event or rights request

- 01 Create a factual inventory of personal data, systems, purposes, locations, processors and transfer routes.
- 02 Provide relevant privacy notices and ensure data access is limited by role.
- 03 Log and handle access/correction or other applicable requests within relevant law.
- 04 Review retention, secure disposal, incident response and processor agreements using actual implementation evidence.

4 Responsibilities and evidence

Accountable process owner. Data Protection / Records Owner maintains implementation, staff guidance, case processing and reporting. Academic decisions requiring external award authority must be referred according to the verified programme arrangement.

Minimum evidence. Processing register; vendor list; privacy notices; access logs; rights-request log; retention schedule.

Record protection. Keep case files, decisions and correspondence in access-controlled systems; apply an approved retention schedule and document transfers to relevant partners. Do not publish personal or confidential records.

5 Exceptions, concerns and review

Exceptions. Material deviations require a written rationale, authorization by a role with the appropriate delegation, and a record of any impact on students or staff. No local exception may override mandatory law or a controlling awarding-body requirement.

Challenge and escalation. Explain the applicable complaints, academic appeals or rights-request route to affected persons. Refer safety concerns, integrity incidents, data incidents, conflicts of interest or disputed award claims to the designated specialist authority.

Monitoring. Audit the website's actual forms, cookies, system integrations and retention practice.

6 Linked institutional controls

Related controls, where relevant: Academic Regulations (ACD-001); Academic Integrity (ACD-003); Student Complaints (STU-004); Academic Appeals (STU-005); Quality Assurance (QUA-001); Privacy and Student Records (DIG-001); Academic Partnerships and Award Information (PAR-001).

7 Document information and periodic review

Document series	IEU Regulations & Policies
Institution	International European University (IEU)
Applicability	See section 1 and programme-specific terms
Student enquiries	Use the IEU contact and support routes
Document maintenance	Controlled by the responsible function