Student Records Management Policy

GC Academy Limited

A25

Revision date 9 September 2026

Institutional approval pending

This policy governs the collection, use, protection and preservation of student records throughout the student lifecycle. It connects admissions, agreements, assessment, progression, support and case decisions to an accurate central academic record, while restricting access to sensitive evidence.

GC Academy retains responsibility for its records when academic or technical work is performed by a partner. The procedures require traceable decisions, reliable access to essential academic evidence and documented retention and disposal. Approval, implementation checks and actual student records are recorded separately from this policy revision.

Contents and policy control

Central records and responsibilities....3
Admissions agreements and acknowledgements....4
Assessment evidence and result history....5
Final Projects and presentations....6
Engagement support and progression....7
Integrity complaints and academic appeals....8
Financial support and institutional information....9
Recording and digital evidence controls....10
Storage security and continuity....11
Retention archiving and disposal....12
Student rights quality review and release....13
Student record action and verification....14
Retention custody and readiness record....15

1 Purpose and application

A25 applies to applicants, enrolled students and graduates, and to every member of staff, committee member, external reviewer and service provider handling their records. It covers paper and digital records, the LMS, linked repositories, authorised communications, exports, working copies, backups and archives.

The Head of Student Management and Administration coordinates the central record. The Head of Quality Assurance Office owns the policy and annual review. The Head of Institution and Academic Board oversee academic provisions. The Director of Operations confirms operational and supplier arrangements; corporate approval follows A16. Actual approval and delegated responsibilities are recorded before use.

The policy operates with A5 Data Privacy and Usage Policy, A14, A16, A17, A18, A1 to A4, A10, A12, A23, A24, the Student Agreement Template, AI Guidance and the applicable assessment rubrics. A25 specifies records and controls; the relevant procedure determines the substantive decision.

Approval reference and effective date: _____

Responsible owner and next annual review: _____

Central records and responsibilities

2 An authoritative student record

Administration assigns a unique student identifier and maintains an authoritative index linking the student, programme and cohort to controlled academic and administrative records. Each record identifies its category, creator, date, source, applicable document version, status, authorised location, access group and retention entry. Record the event date separately where entry occurs later; explain a correction or late entry.

The central record can link to a restricted case or evidence repository. It does not require every file to be copied into a single folder or made visible to every user. Preserve the relationship between records when files are moved or archived. Reconcile duplicate entries against source evidence and retain the necessary correction history.

A blank form, test record, planned meeting or draft decision is labelled accordingly. Only an actual event is marked completed. Identify imported data and its source; check accuracy, completeness, identifiers and permissions before accepting it as an institutional record. An affiliated academy demonstration is not evidence of a GC Academy student event.

3 Accountability and authorised access

Administration maintains admissions, agreements, status and support records and coordinates requests. Tutors and allocated academic staff record submissions, assessment, feedback and relevant academic support. The Head of Institution checks academic completeness; the Board of Examiners validates results, progression and completion under A17 and A18. Technical access does not confer authority to alter an academic decision.

The Head of Quality Assurance Office checks record quality and follow-up. The QA and Curriculum Committee reviews findings; Academic Board considers academic actions. The Director of Operations exercises institutional oversight of technical and financial services. Technical staff implement approved security, backup, recovery and access arrangements and supply evidence for institutional review.

Access is limited to the purpose and assigned role. Administration approves routine administrative access within recorded authority; academic access is confirmed by the Head of Institution. Restricted case access follows its appointed decision-maker and privacy requirements. Financial staff see necessary financial records; tutors receive agreed support adjustments without unnecessary diagnostic evidence. External reviewers receive only the evidence needed for their remit.

Record the named user, authoriser, purpose, permissions, start and review or end date. Use individual accounts; log privileged access and changes. Review permissions when duties or contracts change and remove access when no longer needed. Before access, personnel receive relevant data-protection training and confidentiality instructions. Record actual completion and remedial follow-up.

Admissions agreements and acknowledgements

4 Admission and registration evidence

Retain the application, identity and contact information needed for admission, entry qualifications, verification results, admission decision and notice. Record the programme specification used, cohort, enrolment date, recognition or credit decision where applicable, and any conditions still to be met. Correct an inaccurate personal detail through a documented route without rewriting the original academic decision.

Where a recruitment agency performs preliminary checks, retain the source and verification evidence and identify the Academy officer who makes or confirms the institutional admission decision. Agency access is confined to its agreed role; it does not include unrestricted assessment, wellbeing or case records. The Academy retains custody and access independently of the agency relationship.

5 The signed agreement and actual documents supplied

For A12 and the Student Agreement Template, link the agreement identifier and version to the actual programme and financial schedules and attachments supplied to the student. Retain academic and financial checks, issue date, both parties' identities and genuine signatures, signature dates, and the copy supplied to the student. Record verification that both signatures precede any payment made by or on behalf of the student and programme commencement.

Preserve the terms applicable to that student. A later policy upload does not silently replace a signed contract. Record an authorised amendment, the documents communicated and any required agreement. A draft fee rule, placeholder attachment or unconfirmed approval is not recorded as a completed contract check.

6 Separate acknowledgement and consent records

Link the completed A3 acknowledgement, whether signed or identifiable through the LMS, to the student identifier, confirmation date and method, recording staff member and exact versions of A3, A4, A1, A23 and AI Guidance made available. Retain clarification requests, access assistance and follow-up. After a material change requiring renewed acknowledgement, record the actual renewed confirmation and version supplied.

An acknowledgement of policy receipt, a task-specific AI declaration and recording consent are separate records. Acceptance of general rules does not establish consent to identifiable webinar recording or permission for unrelated data use. Record any required recording consent with the notice and scope described in A24; retain task-specific declarations with the relevant submission.

Record the actual orientation activities completed, guidance supplied and unresolved access or support issues. Do not equate a published guide or a test account with a completed student orientation. Supply accessible confirmation and retain evidence that the student can obtain the applicable documents and support contacts.

Assessment evidence and result history

7 Linking assessment to learning outcomes

For each module and assessed component, link the approved curriculum and learning outcomes to the issued brief, assessment method, rubric version, criteria, weights and published deadline. Retain the individual submission or other authorised evidence, receipt date and method, task-specific AI declaration where required, and any accepted alternative submission or adjustment.

The assessment record preserves each criterion rating and weighted score together with the assessor’s reasoned observations. Evidence of achievement of the intended learning outcomes is recorded separately and linked to the relevant work. An aggregate mark, attendance count or LMS engagement score alone does not establish attainment of every outcome.

For assignments and case studies, retain the actual brief or case, sources and student work considered, criterion-level judgement, calculation and outcome evidence. For group work, identify participants, the shared product and each student’s contribution and individual evidence. A common group product does not replace individual attainment evidence where the assessment requires it.

8 Marking moderation and validation

Preserve the first assessor’s judgement and date, the independent second assessment where required, moderation findings, any disagreement and its resolution, external review where applicable, and Board of Examiners validation. Identify each reviewer and their role. Retain feedback, the date it was released and the version communicated to the student. Do not overwrite the first mark with a moderated or final mark.

Every authorised change identifies the previous and new value or status, affected component and attempt, reasons and evidence, decision-maker and authority, decision date, implementing staff member and actual entry date. Link the relevant moderation, mitigation, misconduct or appeal decision and subsequent student notification. A decision to review a mark is not itself a replacement mark.

The record uses the common evidence requirements in the Assignment Evaluation Rubric, Case Study Evaluation Rubric, Presentation Evaluation Rubric and combined Assessment Rubrics for Assignments and Case Studies. Store the completed assessment record or a controlled equivalent with all required fields. An empty rubric is not completed assessment evidence.

9 Attempts and academic standing

For the BA, record each formal opportunity by module, component, attempt number, scheduled and actual date, outcome and authorising decision. The approved rule is three total formal assessment opportunities, comprising the initial opportunity and two further attempts. Any decision about a disrupted or deferred assessment records how the attempt is treated; staff do not silently reset the count.

Record the applicable 51% pass threshold for each required component and the resulting module outcome under A18. Do not use an overall average to conceal a failed required component. Preserve both validated results and any provisional status pending a case, mitigation or review.

Final Projects and presentations

10 Project development and supervision

The Final Project record links the approved proposal, intended outcomes, project brief and rubric, allocated supervisor, relevant permissions and submitted work. Retain the supervision plan, including the minimum three scheduled consultations under A18, actual meetings, feedback, agreed actions and any intervention or escalation. Distinguish a scheduled consultation from one that took place and record follow-up after a missed meeting.

The supervisor records guidance and progress without treating it as the final assessment decision. Changes to topic, scope, deadline or arrangements identify the request, academic authority and approval. Keep sensitive information in the appropriate restricted record, linking only the necessary decision or agreed adjustment to the academic file.

11 Presentation and defence evidence

For an assessed presentation or defence, record the student and group members where relevant, date, mode, actual duration, assessors, any external reviewer and other authorised participants. Link the presentation materials and rubric versions, individual observations, questions and responses, and evidence addressing the intended outcomes. Record an authorised recording only where the assessment and privacy arrangements permit it.

Capture the original assessment, independent second judgement where required, moderation, external comments and final validation. A presentation record includes enough reasoned evidence to support the judgement even where no video is retained. A recording is not substituted for the assessor’s criterion-level reasons and feedback.

A technical interruption, identity concern or access adjustment is recorded with its timing, effect, support action and authorised academic response. Retain the original evidence and the decision on completion, continuation or rescheduling. An interruption or proctoring alert does not by itself establish misconduct or consume an additional attempt.

12 External input and completion

Link the appointment and remit of external academic or professional reviewers to their actual contribution to preparation, review or assessment. Retain relevant qualifications or appointment checks in the controlled staff or governance record, with a reference in the project file. Record conflicts, access permissions, the report received, institutional consideration and resulting action.

The Board of Examiners validates results and completion using the assessment evidence. Academic Board confirms award eligibility within A17. Administration records the validated outcome, award decision, issue date and identifier of the transcript or certificate, and any subsequent correction or replacement. Preserve prior issue details and the authority for a change.

Do not record an external review, defence, award or signature as completed merely because a template or appointment plan exists. Preserve the evidence supporting the actual event and its connection to the student’s final academic record.

Engagement support and progression

13 A documented response to students at risk

LMS activity data supports early identification of students who may need assistance. Retain the relevant event, date range and source, the reason for the alert and the staff member who checked it. Consider technical faults, authorised absence, offline work and agreed adjustments before interpreting an apparent lack of activity. An automated flag is neither an academic judgement nor a termination decision.

Administration opens a linked support entry and allocates a responsible person. Record each attempted and successful contact, date and channel, student response, identified barrier, agreed action, responsible academic or administrative staff, deadline and review point. Preserve relevant communications received outside the LMS in the controlled record.

An unresolved academic issue goes to the responsible tutor and Head of Institution; an operational or technical issue goes to the relevant administrative lead and, where necessary, the technology provider. Record the referral, recipient, date, required action and follow-up. Escalate overdue or ineffective action to the competent institutional authority and QA for process monitoring. A sent message alone does not establish resolution.

Track the first-response target of 24 hours during business hours separately from resolution time and any formal decision deadline. Record acknowledgement, substantive response, outstanding work and cover during staff absence or overlapping intakes. A case closes only when its outcome and any continuing support have been recorded.

14 Module deadlines inactivity and return

For each module, record the individual registration date and the corresponding 12-month completion deadline, together with any authorised amendment. This is not a 12-month limit for the entire BA. Preserve the original and revised date, reasons, authority and student notification.

The BA inactivity review uses 90 calendar days, with the relevant engagement dates, previous contacts, support offered, warning and student response recorded. It triggers an individual review of status under the academic rules. It does not authorise automatic expulsion, cancellation of all achieved credits or a full programme restart.

For approved suspension or interruption, retain the reasoned decision, effective dates, module and attempt position, support arrangements and communications. The return plan supports rejoining in the following semester and records the actual modules available, dates, retained achievements, remaining attempts, adjustments and any effect on the intended graduation date. Communicate and follow up the agreed plan.

Withdrawal, termination, progression or reinstatement records identify the competent decision-maker, reasons, applicable procedure, effective date and review or appeal route. Administration implements the authorised decision and verifies the resulting record. Financial consequences are recorded separately under A10; neither an unpaid balance nor an inactivity alert silently changes an academic result.

Integrity complaints and academic appeals

15 A linked and restricted case record

For a student ethics, digital conduct, misconduct or complaint case, retain the report and original receipt date, applicable policy version, allegation or issue, relevant evidence, notices, student response and support or representation. Link the case identifier to the central record while keeping sensitive evidence in a restricted repository. Staff or supplier cases are not copied into a student file without a necessary student-related purpose.

Under A4 and AI Guidance, record the actual brief and permitted AI use, declaration, material reviewed, detector limitations, human examination and the student's explanation. A similarity score, AI output or platform alert is evidence to examine, not a finding. Preserve relevant original evidence and its source; do not add an unsupported allegation to a validated result.

The case file links appointments, independence and conflict checks, the three independent academic voters where required by A4, non-voting procedural support, evidence considered, majority decision and reasons. Record notice, sanction or other authorised outcome, the appeal route and any protective restriction separately. Interim protection is not a completed misconduct sanction.

16 Academic appeals and implementation

Maintain the records required by A1 Annexes 1 and 2: the challenged decision and notice date, original appeal receipt, the ten-working-day submission deadline, grounds, evidence, any accepted timing exception, appointment and conflict checks, student response and the reasoned outcome. Track the normal fifteen-working-day outcome period under A1 and record any communicated exception or revised date.

Retain the independent panel's appointment and decision record, including its three eligible voters and majority outcome. The original decision-maker does not determine the appeal. Link the resulting remedy to the Board of Examiners or other competent authority for implementation, identifying the old and new result or status and the date of student notification.

A4 Annexes 1 and 2 and A1 Annexes 1 and 2 supply the detailed case and decision fields; a controlled equivalent must preserve them. Record only actual steps. A promised review, blank panel form or proposed sanction is not a completed case or implemented result change. An appeal remedy does not silently create a fourth assessment attempt.

17 Closure and confidentiality

A2 governs service complaints; mixed issues are linked and routed without losing receipt dates or deadlines. The case record identifies the decision, communications, implementation, outstanding action and closure authority. Record any further review and the relevant retention or legal hold. Restrict access to those who need the evidence for fair consideration; give the student the information required to respond while protecting other people's data.

Financial support and institutional information

18 Fees and refund records

Administration links financial records to the student and signed agreement; the Accountant maintains the payment and reconciliation evidence. Retain the applicable A10, agreement and financial-schedule versions, charges, invoices, receipts, instalment arrangements and authorised amendments. Do not infer a scholarship, payment or agreed exception from a blank field or proposed scheme.

For a refund, preserve the original request receipt, relevant dates, necessary evidence, calculation, applicable rule, decision authority and date. Track the ten-working-day decision target from receipt and the thirty-working-day payment target from the decision, with any reasoned delay and revised date communicated to the student. Record the approved amount, verified recipient, payment reference, actual payment or failure, reconciliation, notification and closure.

Approval is not payment. A failed transfer stays open for follow-up. Financial decisions and their authority remain separate from academic decisions, results and attempts. Keep medical or other sensitive evidence supporting an exceptional request restricted; the general ledger needs the financial decision and appropriate reference, not the full private history. A25 records the approved terms used; it does not select unresolved commercial refund terms.

19 Personal support and adjustments

Record the support requested, agreed adjustment, responsible staff, implementation and review in the student’s central record. Restrict diagnostic or professional evidence to staff who need it. Tutors receive the functional arrangements necessary for teaching and assessment. Record an actual referral and follow-up accurately; providing wellbeing information or an external contact is not evidence that professional counselling took place.

Where an Individual Learning Support Plan is used, identify its version, agreed measures, permissions, responsible persons and review date. Communicate changes to relevant staff and retain confirmation of implementation. A planned service, referral pathway or adjustment is not marked available or completed without supporting evidence.

20 Statistics feedback and graduate information

Maintain reliable participation, retention, completion and success information with defined reporting periods, cohort populations and calculation methods. Student profiles, including information about vulnerable groups where necessary and lawful, are protected against unnecessary identification. Record survey versions, response dates and coverage; report response rates and limitations. Do not present non-response as satisfaction.

Employment and career information, where relevant to the programme, identifies its source and collection period. Alumni community access and digital-library use are distinct from academic record retention. Continued access does not itself demonstrate employment outcomes or consent to publicity or unrelated contact. Use appropriately aggregated or anonymised information for routine quality review and link findings to actual decisions and follow-up actions.

Recording and digital evidence controls

21 Separate categories and permissions

A24 distinguishes prepared lecture resources, semester webinars, other online teaching and meetings or administrative events. Assessment submissions, recorded presentations and proctoring evidence are separate evidence categories. The record identifies the purpose, legal basis, audience, responsible person, notice, permissions, file version and applicable retention or removal rule before capture or publication.

The webinar register links the semester, title, tutor, eligible cohort, notice, cleared file, publication date, permissions check, planned removal and actual removal. Keep participant-level consent and non-recording arrangements in a separate restricted record. General acceptance of A3, A12 or platform terms does not replace informed recording consent required by A24.

Document any withdrawal of consent, accidental capture, restriction, editing or other required action and the response sent. Retain a reference to the actual notice and its version. Do not promise recall of every downloaded copy. Privacy requests follow section 28 and A5, with relevant recipients informed where required.

22 Removal and exceptional preservation

Semester webinar copies are removed from the LMS at semester end before the next cohort receives access, as specified in A24. Record the responsible person, planned and actual removal dates, location and verification. Eligible students' permitted personal-study copies are distinguished from institutional copies. Prepared lecture resources follow academic review and replacement and are not automatically deleted at semester end.

LMS removal does not prove deletion of working files or backups. Technical staff identify these copies and apply the recorded retention and backup cycle, restricting access and preventing routine republication of expired webinars. Record the actual disposal or scheduled backup expiry and verify the action when it occurs.

An institutional recording needed for an actual appeal, complaint or other justified requirement is separated from ordinary learning resources. Record the case, purpose, decision authority, access group, retention reason and review or disposal point. Review and release the hold when the reason ends. A generic reference to quality assurance does not justify indefinite storage.

23 Assessment and identity evidence

For presentations, identity checks and proctoring, retain only evidence necessary for the approved assessment, integrity and review purposes. Identify the assessment, student, capture method, notice, incident if any and authorised reviewer. Apply the specific retention entry; do not automatically use the webinar semester-removal rule or the 40-year period for every raw recording or image.

Preserve sufficient proof of assessment in the academic archive and any evidence needed for an open case. Document why a raw file remains necessary or how the required evidence is preserved in a more limited record. Access to sensitive captures is restricted and recorded; raw files are not ordinary downloadable learning materials.

Storage security and continuity

24 Approved locations and institutional custody

The storage design specifies EU-based primary hosting in Hungary and secure archival provision in Malta. Before student records depend on these arrangements, the Director of Operations and technical staff verify and document the actual provider, locations, systems, responsible custodian, contract and access arrangements. Record changes and institutional approval. The location description alone does not establish GDPR compliance or a tested archive.

GC Academy maintains, retains and archives the required student records in Malta and keeps essential academic records readily available for 40 years. The Malta archive record identifies its location, access authority, protected copies, recovery arrangements and retrieval test evidence. An overseas live server or an unverified backup label does not demonstrate the Malta archival requirement.

Technical staff apply encryption, controlled access, secure transfer and monitoring proportionate to the information held. Record the implemented controls and checks. Protect identifiers and evidence when staff work remotely; restrict local exports and securely remove temporary copies according to the schedule. Keep any necessary paper originals in controlled physical storage with a custody record.

25 Suppliers backups and incidents

Supplier agreements define documented instructions, confidentiality, security, authorised personnel and subprocessors, incident escalation, assistance with rights requests, access for institutional checks and return or deletion at service end. Identify any international disclosure or remote access and confirm the applicable transfer safeguards. A confidentiality clause alone does not establish all necessary processing arrangements.

The Academy retains usable records and export rights independently of the LMS supplier. Source-code ownership does not replace record custody, recovery or exit arrangements. The Director of Operations arranges institutional scrutiny of service evidence and conflicts under A16 and A23; the supplier or a person overseeing their own implementation does not solely verify compliance.

A14 and the actual service arrangements specify backup and recovery operations. Technical staff log completed backups, failures, remedial actions and restoration tests, checking that student identifiers, submissions, mark history, case links and permissions survive recovery or migration. Keep protected copies separate from the live system and verify archive retrieval and readable formats over time.

Report loss, unauthorised disclosure or alteration immediately through the institutional incident route. Preserve evidence, restrict further exposure and record discovery, affected data, containment, responsible persons, risk assessment and required notifications. Privacy and incident leads assess statutory notification duties under GDPR Articles 33 and 34 without waiting for the ordinary support or committee cycle.

On service interruption, supplier change or institutional cessation, A14 governs the authorised continuity response. Record the handover, receiving custodian, lawful access and contact route, complete inventory and verification. Preserve students’ ability to obtain essential academic records; do not mark a planned migration or recovery test as completed.

Retention archiving and disposal

26 A controlled retention schedule

The schedule identifies each record category, purpose and applicable requirement, authoritative location, custodian, access group, retention period or justified criterion, event starting the period, calculated review or disposal date and approval. The Head of Quality Assurance Office coordinates it with Administration, the Head of Institution, Operations and the privacy function under A5. Complete the applicable entry before collecting or releasing a new category of records.

Essential academic records, including proof of assessment, validated results, transcripts and completion certificates, remain readily available in Malta for 40 years. Specify the records necessary to evidence admission, achievement and award and the applicable retention trigger in the schedule. Verify the trigger against the governing requirement; do not shorten the 40-year provision or dispose of a protected academic record while its requirement remains unresolved.

The following categories require separate entries. The schedule does not impose a blanket 40-year retention period on all underlying personal data:

- Admissions and agreements: retain the necessary admission and contractual evidence, document versions and acknowledgements for their academic, contractual and applicable legal purposes; remove unnecessary duplicate identity material when its purpose ends.
- Assessment working material and case evidence: preserve sufficient academic proof and evidence needed for marking, moderation, appeal or a justified hold. Record a separate period for raw captures and unnecessary duplicate submissions.
- Support and sensitive evidence: retain the necessary decision and implemented adjustment, with a separately justified period and tighter access for diagnostic or professional material.
- Financial records: use the applicable accounting, contractual and legal requirements for transactions, refund calculations, decisions and payment evidence; distinguish restricted supporting evidence.
- Activity logs, surveys, alumni information and recordings: use their notified purpose and specific rule. A24 governs webinar LMS removal; backup expiry, consent evidence and exceptional case copies remain separately traceable.

27 Archive checks and lawful disposal

Review the schedule and archive at least annually and after material change. Check completeness, readable formats, permissions, retrieval, redundancy and recovery evidence. Record migration checks and correct broken links or unreadable files. A backup is not a substitute for an indexed long-term archive.

Before disposal, the custodian checks the due date, requirement and any active complaint, appeal, regulatory request or legal hold. Record a hold’s reason, scope, authority and review date; retain only what it covers. Once lawful disposal is authorised, record the category, date range, method, responsible person, actual completion and verification, including treatment of copies and backup expiry.

Use secure deletion, destruction or effective anonymisation as appropriate. Keep a minimal disposal record without retaining the deleted content. A withdrawal, failed assessment, inactive account or request for erasure does not automatically delete academic achievements or override a necessary lawful retention requirement.

Student rights quality review and release

28 Access correction and privacy requests

Students use the confirmed institutional privacy route under A5 to request access, correction or other applicable data-protection action. Administration records the original receipt and promptly routes the request to the responsible privacy contact. A request received through a general support channel is not discarded or given a new receipt date on referral. Verify identity proportionately where necessary and protect other people's information in any disclosure.

The Academy responds without undue delay and within one month of receipt. Where complexity or the number of requests justifies an extension, it informs the requester within that month, explains the reasons and records the revised deadline, which may extend by up to two further months. Record the action or reasoned refusal and information about the right to complain to the Information and Data Protection Commissioner and seek a judicial remedy.

Rights, including erasure, restriction, objection and portability, apply under their respective legal conditions. Explain any necessary lawful retention rather than promising automatic deletion. Correct inaccurate personal data through a traceable process. A disputed academic judgement follows A1; a privacy request is not treated as authority to remark work or erase a valid award history.

29 Monitoring and annual review

QA and technical staff conduct an annual records audit with Administration and academic input. Check a proportionate sample from admission to award or withdrawal, including assessment evidence, grade changes, support escalation, cases, access permissions, retention and recovery. Record findings, limitations, responsible owners, action dates and evidence of correction.

The QA and Curriculum Committee considers findings and effectiveness; Academic Board receives academic issues and the Director of Operations and Board of Directors receive relevant operational risks. Track overdue action and verify its outcome before closure under A17. Following the first delivery cycle, review support response and resolution times, student feedback and engagement patterns using actual records.

The Head of Quality Assurance Office reviews A25 annually and following relevant legal, institutional or programme change. Academic amendments receive Academic Board approval; corporate or resource decisions follow A16. Retain approval, effective date, superseded version and evidence of communication to affected staff and students. Record training and follow-up required by the change.

30 Before operational use

Confirm named custodians and contacts, role permissions, privacy notices, completed retention entries and actual storage and supplier arrangements. Test an end-to-end record using clearly labelled test data, including an authorised correction, support escalation, archive retrieval and restricted access. Record results and unresolved actions. A policy, form or demonstration alone does not establish that the programme is operational or these checks have passed.

Student record action and verification

Appendix A Controlled entry or linked record

Complete for an actual event or authorised change. Equivalent controlled system fields may be used. Reference the specialist assessment, case, support or refund record instead of duplicating sensitive evidence. Label tests and drafts explicitly.

Student identifier programme and cohort: _____

Record category event or case identifier: _____

Event date receipt date and entry date: _____

Source and applicable document versions: _____

Authoritative location and linked evidence: _____

Record owner and authorised access group: _____

Action or decision and reasons reference: _____

Decision authority and actual decision date: _____

Previous and new value or status if changed: _____

Affected module component and attempt: _____

Action owner deadline and escalation route: _____

Student response and notification reference: _____

Implementation date and responsible person: _____

Verification result reviewer and date: _____

Outstanding action next review or closure: _____

Retention entry and any restricted case link: _____

Completeness and use

Confirm that the linked evidence supports the entry, the competent authority made the decision, required notice was given and the actual implementation agrees with the outcome. Preserve the earlier value and source. Record an unresolved discrepancy and its owner rather than marking the record verified.

For support, retain each contact and review; for assessment, retain criterion and outcome evidence and all required marking stages; for a case, retain the relevant A1 or A4 annex fields; for a refund, retain the A10 receipt, calculation, decision and payment trail. This control sheet does not replace those detailed records.

Retention custody and readiness record

Appendix B Category and archival control

Use one entry per category or defined archival collection, with linked supporting schedules where needed. Complete actual arrangements and approvals; a blank entry is not evidence of operational readiness.

Category purpose and applicable requirement: _____

Custodian location and authorised access: _____

Period or criterion and starting event: _____

Review or disposal date and approval: _____

Live copies archive and backup locations: _____

Retrieval or restore test date and evidence: _____

Hold reason authority and review if applicable: _____

Disposal method completion and verification: _____

Release and periodic verification

The policy owner records confirmation of the actual privacy contact, custodians, access matrix, current notices, retention schedule and supplier controls. Operations verifies hosting and Malta archival evidence; academic staff verify assessment and decision records. QA records test results, unresolved issues and follow-up. The approval record states when the policy takes effect.

Verified arrangements and evidence references: _____

Open action responsible person and due date: _____

Institutional approval and effective date: _____

Communication training and review record: _____

External reference points

MFHEA E-Tool, indicator 4.8: student records in Malta and 40-year availability of academic records. https://mfhea.mt/e-tool/

Regulation (EU) 2016/679, particularly Articles 5, 12 to 22, 28, 32 to 34 and Chapter V: processing principles, rights, processors, security, incidents and international transfers. https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng

Information and Data Protection Commissioner, Your Rights: requests and available remedies. https://idpc.org.mt/for-individuals/your-rights/