

Digital Conduct and Use Policy



A24

GC Academy Limited

Recording arrangements and responsible use of digital services

Revision date 9 September 2026

Institutional approval pending

This policy explains how students, staff and other authorised users participate safely and respectfully in the Academy's digital environment. It distinguishes continuing lecture materials from semester webinar recordings and sets out notice, consent, access, download and removal responsibilities. Concerns about digital conduct receive human review and the appropriate institutional procedure.

Contents and document control

Scope and recording categories.....	3
Recording notice and participation.....	4
Access downloads and removal.....	5
Responsible use and ownership.....	6
Reporting and fair decisions.....	7
Review and readiness for use.....	8
Webinar register record.....	9

Status and responsibility

This revision updates the existing A24 Digital Conduct and Use Policy. References to the Digital Learning Code of Conduct in the accreditation response identify this same document. The revised text is prepared for institutional approval; the revision date does not establish approval, publication or programme delivery.

The Head of Institution owns the policy. The Head of Quality Assurance Office coordinates review and document control with Administration and technical staff. The QA and Curriculum Committee reviews proposed improvements; Academic Board approves academic provisions under A16 and A17. The Director of Operations confirms operational responsibilities and authorised supplier arrangements.

Approval reference and date: _____

Effective date and next review: _____

Related procedures

Read A24 with A23 Code of Ethics and Professional Conduct, A4 Academic Integrity and Misconduct Policy, A1 Academic Appeals Procedure, A2 Complaints and Grievances Procedure, A3 Academic Integrity Acknowledgement and the existing AI and Generative AI Guidance for Staff and Students.

Recording and access information must agree with A12 Student Learning Agreement, the Student Agreement Template, A25 Student Records Management Policy, the Data Privacy and Usage Policy, LMS onboarding guidance and the online identity verification and examination proctoring procedures. A14 Business Continuity Plan and the actual technology-provider agreement govern the relevant technical arrangements.

The data-protection provisions are read with Regulation (EU) 2016/679, in particular Articles 5 to 7, 13 and 17. Official text: <https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng>

The approved current version and reporting contacts are communicated before use. Keep superseded versions identifiable. Approval, publication, staff preparation and actual student acknowledgement are recorded separately when they occur.

Scope and recording categories

1 Introduction

GC Academy requires respectful, secure and responsible use of its digital services. Users protect other people's contributions, personal information and intellectual property. Recording has a defined purpose and audience; access to a platform does not authorise every use of its content.

2 Scope of application

This policy applies to students, academic and administrative staff, affiliates, partner personnel and other authorised users of the LMS, institutional email, forums, chat, file repositories and associated services. It applies when creating, sharing, downloading, storing or reusing institutional material, including use on personal devices.

3 Recording of sessions

Recording arrangements depend on the activity. There is no blanket rule that all lectures, meetings, training events or synchronous activities are routinely recorded. Identify the category before recording and apply the notice and permission requirements on the following pages.

3 1 Recorded lectures

Prepared lecture recordings form part of the continuing programme learning materials. They remain available to the relevant students through the LMS and are not deleted automatically at semester end. The responsible academic staff review, update or replace them through programme monitoring. Confirm presenter and content permissions before release; any identifiable student contribution needs specific consideration.

3 2 Semester webinars

Live webinars provide additional interactive academic support for the students enrolled in the relevant semester. Their recording lets that cohort revisit explanations or access a session missed live. Recordings focus on the tutor, presentation and teaching material; student participation follows section 3 5. The cohort may download recordings for personal educational use. The LMS copy is removed at semester end, as set out in section 3 7.

3 3 Other online teaching activities

Other synchronous teaching, discussion or training activities are not routinely recorded. Any proposed recording requires a defined purpose, responsible organiser, informed participants, the appropriate consent and privacy arrangements, and a stated audience and retention decision before it starts.

3 4 Meetings interviews and administrative events

These events are recorded only for a defined purpose, with prior notice, informed consent of participants and the applicable data-protection arrangements. They do not acquire webinar download permissions. Assessment submissions, recorded presentations and identity or proctoring evidence follow the approved assessment and specialist procedures; they are not ordinary webinar resources.

Recording notice and participation

3 5 Informing participants and obtaining consent

Before capture, the organiser confirms the purpose, applicable legal basis and retention arrangements through the Data Privacy and Usage Policy. The organiser provides clear information before the event and the tutor announces recording again when it starts. Late arrivals receive the same information before an identifiable contribution is captured. The notice identifies:

- The activity, purpose, responsible organiser and what is captured, including any image, voice, name, chat or screen content.
- The intended viewers, where access is provided, any download permission and the applicable retention or LMS-removal point.
- How to participate without being identifiable in the recording, how consent is recorded where required, and whom to contact about privacy or withdrawal.

For a webinar, explain that eligible students may download and retain the recording permanently for personal study and that removal from the LMS does not remove downloaded copies. This information precedes any consent to include an identifiable student contribution.

Students need not activate their camera or microphone for ordinary webinar participation. Before including an identifiable contribution, obtain an informed, voluntary and recorded agreement covering the stated recording and sharing. Silence, joining the session, a camera setting or acceptance of A3, A12 or general platform terms is not that agreement. Refusal does not attract a penalty in webinar participation.

A practical opportunity not to be recorded

The tutor offers a non-recorded question or contribution route, such as private messaging followed by an anonymised question, a pause in recording or an agreed follow-up discussion. Do not display names, participant lists or private chat in the recording. A camera being off is insufficient if a voice, name, chat or screen share still identifies the student.

The tutor and technical staff check the capture settings beforehand. If they cannot exclude a non-consenting contribution, pause or stop capture and agree an appropriate alternative. Accidental capture is restricted from release until the contribution is removed or appropriately anonymised and the corrected version is checked. Do not promise a feature that has not been tested.

For assessment or identity checks, explain the separate approved requirements and support route in advance. A webinar camera choice neither waives those requirements nor permits an undisclosed assessment recording. Consider access and support needs through the applicable procedure.

Privacy questions and withdrawal

Where processing relies on consent, a participant can withdraw it through the stated institutional contact as easily as it was given. Withdrawal does not undo earlier lawful processing. Administration routes the request through the Data Privacy and Usage Policy and records the action, including restriction, editing or deletion where required. Explain any applicable retention reason and the response to the requester.

The Academy cannot promise technical recall of every copy already downloaded. It addresses affected institutional copies and informs relevant recipients of required action where applicable. Download permission does not remove privacy rights. Keep consent records separate from the recording and accessible only to authorised staff.

Access downloads and removal

3 6 Checking and releasing the recording

The tutor checks that the final webinar file matches its stated purpose and contains only authorised material. Administration verifies the semester, eligible cohort, file version, notice and consent record and tutor clearance before publishing. Technical staff configure access for the authorised cohort and the staff who need it. Test access and download permissions; do not rely on an untested default.

Students in that cohort may download the webinar recording and retain it permanently for personal educational use, subject to the stated rights and privacy requirements. They must not redistribute it, republish it, sell it, use it commercially or make it available to people outside the cohort. A public link, shared login or upload to an external service is not authorised by the download permission.

Access is for the relevant semester cohort, not a future intake. Teaching recordings, meeting records and assessment evidence have their own authorised audience. Reuse for another purpose, cohort or public communication requires a separate content, rights and privacy review before release.

3 7 Removing the semester webinar copy

Administration removes the webinar recording from the LMS at the end of the relevant semester and before the learning area is prepared for a new cohort. Record the planned removal date and the actual removal and access check. A new webinar and recording is produced for the next cohort where required. Continuing lecture materials follow section 3 1 instead.

LMS removal does not affect permitted copies already downloaded by eligible students. It also does not prove erasure from every institutional working file or backup. Technical staff identify such copies and apply the approved retention and backup cycle, with restricted access and no routine republication of an expired webinar.

An institutional copy retained for an actual complaint, appeal or other documented requirement is separated from the learning resource. Record the purpose, authorised access, applicable retention reason and review or deletion point under A25 and the Data Privacy and Usage Policy. A general reference to quality assurance does not authorise indefinite retention. Record completed disposal when it occurs.

3 8 Responsibilities and the webinar register

The Head of Institution oversees academic suitability and resolves escalated delivery issues. The tutor manages advance notice, consent for identifiable contributions, participation alternatives and content clearance. The Head of Student Management and Administration coordinates cohort publication, queries, the webinar register and semester removal.

Technical staff implement and evidence access, download settings and removal or backup actions under the Academy's authority. QA checks that the procedure and records agree and follows up exceptions. Supplier implementation does not replace the independent institutional oversight required by A23.

The register links the semester, webinar title, responsible tutor, authorised cohort, publication date and actual LMS-removal date. It also links the notice, consent or non-recording arrangements, cleared file, permissions check, planned removal and any exception. Use the blank record on page 9 or equivalent controlled fields. Keep participant-level consent evidence outside the general register.

Responsible use and ownership

4 Acceptable use of digital platforms

Use institutional systems for academic or official purposes and communicate respectfully and professionally. Protect passwords, use only your own authorised account, and do not share credentials. Handle learning resources and personal data only for the permitted purpose. Report lost access, suspicious activity or inappropriate content through the current support or reporting route.

Harassment, discrimination, bullying, intimidation and retaliation are prohibited under A23. Preserve relevant evidence and report a concern confidentially rather than circulating personal allegations. Good-faith reporting is protected; an allegation that is not upheld is not, for that reason alone, malicious.

5 Intellectual property and server infrastructure

Teaching materials developed by tutors are treated as Academy property unless otherwise contracted; the actual agreement establishes the relevant ownership and use rights. Check third-party permissions and attribution before sharing. A download permission does not transfer ownership or authorise creative theft.

Student submissions remain the student's intellectual property. Their anonymous use for internal quality assurance requires consent under this policy; teaching, publication or commercial reuse requires the relevant separate permission. Routine assessment and required student-record processing follow their own notified arrangements.

Technical operations maintain controlled access, appropriate security, backups, recovery and incident records under A14, the Data Privacy and Usage Policy and the actual service agreement. Verify service performance from current evidence. Historical provider continuity, uptime or absence of incidents must not be treated as a substitute for monitoring. The Academy retains institutional oversight of its suppliers.

6 Prohibited digital behaviours

- Copying or reusing protected content without permission, or distributing internal learning resources outside their authorised audience.
- Bypassing security, accessing restricted information, impersonating another user or disrupting digital services.
- Plagiarism, fabricated evidence, deceptive attribution, prohibited AI assistance or failure to disclose or cite assistance where required.
- Unauthorised recording or sharing of another person's contribution, confidential material or assessment evidence.

The approved assessment brief and AI Guidance sections 5 to 12 define permitted AI use, disclosure and review. Verify outputs and sources; protect confidential data. An AI tool permission is not permission to upload personal information externally. A3 acknowledgement is neither blanket consent nor a waiver of response or appeal rights.

7 Innovation and commercial use

GC Academy supports ethical development of digital content, educational tools and services. Where a venture arises within an Academy project or programme, define intellectual property rights before exploitation and document any co-ownership and revenue-sharing agreement. Support through mentorship or partnerships depends on the arrangements actually established. No student or tutor acquires a commercial right merely through platform access or participation.

Reporting and fair decisions

8 Enforcement and review

8 1 Reporting and immediate support

Report a digital concern through the published institutional support or reporting channel. Provide relevant dates, activity, affected material and available evidence without sharing unnecessary personal data. QA coordinates confidential triage and identifies the applicable procedure. A23 governs ethical conduct, harassment, conflicts and protection from retaliation; A2 covers general complaints; A4 covers suspected academic misconduct.

A report about the usual contact goes to the alternative unconflicted authority in A23. The person complained about does not control their own investigation. Confidential information is shared only as needed for fair consideration. Any urgent, proportionate protective restriction is recorded separately from a finding or sanction, with an owner and review point; preserve appropriate academic access or an agreed alternative where possible.

8 2 Technical incidents and academic evidence

A technical fault, access problem, proctoring flag, similarity result or AI score does not automatically establish misconduct or justify a penalty. Preserve relevant times, support messages, error details, submission records and system evidence. A platform log alone does not establish authorship or attainment. Both positive and negative detection results have limitations.

Students report access or submission difficulties promptly to Administration and the tutor through an available channel. Staff record the difficulty and arrange an authorised alternative or refer a request for mitigation, timing or assessment arrangements to the competent academic authority. A support response does not itself change a deadline or result; communicate the actual decision and retain the evidence.

For an academic-integrity concern, the assessor examines the approved instructions, work, declaration and contextual evidence under A4. Where a concern remains, the student receives the allegation, relevant rule and evidence in writing and an opportunity to respond before formal referral. The student may provide evidence and request a meeting or appropriate support.

8 3 Independent decisions and appeal

Under A4, three independent academic voters, including a senior academic chair, consider the case and decide by majority. The original assessor, referrer and anyone involved in the merits do not decide it. QA provides non-voting procedural support. The Head of Institution implements the authorised outcome without replacing the Panel's finding. Only authorised, proportionate sanctions apply.

An academic-misconduct appeal goes directly to the independent Appeals Panel under A1 within ten working days of notification. It does not return to the original tutor for informal resolution. Three independent voters decide by majority; previous assessment, moderation, referral, first-instance decision or implementation involvement excludes a person from deciding the appeal.

A1 sets out grounds and remedies, including procedural unfairness, relevant new evidence, inadequate consideration of mitigating circumstances, an unsupported finding or a disproportionate sanction. The written outcome gives reasons within fifteen working days of receipt of the formal appeal; exceptional delay is explained with a revised date. Other academic appeals, general complaints and staff or ethical concerns retain their respective A1, A2 and A23 routes.

Review and readiness for use

8 4 Records and policy review

Administration retains the webinar register and links to the controlled recording records. Student cases follow A25; consent, privacy, staff and supplier records follow their applicable access and retention arrangements. Record the actual event, decision and action, with the person responsible and date. Do not enter a planned action as a completed one.

QA and technical operations review A24 annually and when changes in delivery, technology, privacy requirements or recorded experience require earlier revision. Academic staff contribute findings about participation and learning. Review recording permissions, unrecorded participation, access, downloads, removal, privacy requests, incidents, complaints and staff or student feedback when available.

The QA and Curriculum Committee considers recurring issues. Improvement actions in the Quality Enhancement Log identify evidence, responsibility, due date and expected result; QA verifies completion and effectiveness. Academic Board approves academic changes through A16 and A17. Routine QA monitoring does not reopen an individual decision outside its appeal route.

8 5 Publication and preparation

Before programme commencement, approve and publish the current A24 and align the recording clauses in A12, the Student Agreement Template, LMS guidance and the Self-Assessment Report. Student information states the actual recording categories, download permission, removal point and contact route. Confirm the monitored privacy contact identified under A5 section 5 and include it in the event notice. General acceptance of institutional policies remains distinct from specific recording consent.

Staff preparation under A7 and A21 covers notice, consent, capture settings, participation alternatives, content clearance, cohort permissions, downloads, removal, incident handling and escalation. Administration communicates the current information through induction and the relevant course area and records actual acknowledgement by person, version and date. Follow up missing preparation or acknowledgement.

8 6 Checks before the first webinar

Before the first programme webinar, the tutor, Administration and technical staff test the complete procedure and retain the results. QA checks the evidence and escalates unresolved issues to the Head of Institution. The checks cover:

- Advance and start-of-recording notices, the consent record and an effective route to contribute without being identified in the recording.
- Capture settings, accidental-capture correction and tutor clearance of the published file.
- Access and download by the eligible cohort, exclusion of unauthorised users and the student-facing terms.
- The webinar register, a removal rehearsal, the semester-end action and review of working or backup copies.

A rehearsal is labelled as a test. Actual publication, consent, student access, downloaded copies and semester removal are recorded only after those events occur. Programme-specific student or webinar evidence is not created before the activity exists. Unresolved recording or privacy issues must be resolved before the affected recording is released.

Webinar register record

Appendix A Blank record for one webinar

Administration completes one record per actual webinar or maintains the same fields in the controlled register. Link to restricted consent or case records rather than copying personal details into a broadly accessible list. Use a separate, clearly labelled record for a readiness test.

Record identifier and status: _____

Programme module and semester: _____

Webinar title: _____

Session date and responsible tutor: _____

Authorised student cohort: _____

Recording purpose and cleared file reference: _____

Advance notice and start notice evidence: _____

Consent record or non-recording arrangements: _____

Tutor clearance and date: _____

Access and download check and responsible person: _____

Publication date and LMS location: _____

Planned semester-end LMS-removal date: _____

Actual LMS-removal date and access check: _____

Responsible administrator and confirmation date: _____

Working or backup copy action reference: _____

Exception or privacy request reference if applicable: _____

QA review action owner and due date: _____

The record does not certify consent or completed removal until the supporting evidence exists. Do not record a new cohort as entitled to the previous semester's webinar. Any retention exception identifies its purpose, authorised access and review or deletion point.