Data handling and operations note

What the Foundiro digital workspace stores, who can see it through the application, how access works, which lesson-opening rules apply, and which of these statements have been confirmed by which kind of test. Written for a university's IT, data-protection and programme offices.

The paper programme does not depend on the workspace. A university may deliver Foundiro entirely on paper, or use the workspace for some cohorts and not others.

What the workspace is

A hosted web application run by Foundiro, with the same 84 lessons as the classroom package. Students read lessons, save practice attempts, complete typed worksheets, submit them and receive facilitator feedback. Facilitators see the submitted work of their own cohorts. An operator role manages institutions, cohorts and staff. Access is by invitation only; there is no public sign-up.

Two kinds of access are described below and kept apart: what a person can see through the application's screens and routes, and what the Foundiro operator can reach in the database itself. The database holds everything; the application shows each role only its part.

What is stored, and who sees it through the application

Record	Content	Who can see it in the application
Account	Name; a sign-in email chosen by the person (used as a sign-in name, not verified, no email is ever sent to it); a password hash; a hash of a recovery code the person saves privately	The person. The operator sees name, role and status, never the password or codes
Invitation	A hashed single-use code with an expiry, prepared by a facilitator or the operator and shared in person	The facilitator who prepared it sees it once; it is never shown again or sent by the system
Private lesson record	Saved practice attempts, knowledge-check answers, notes and highlights for each lesson	The student only. No facilitator or operator route reads it
Draft worksheet	The student's current typed worksheet, with the first attempt preserved and a snapshot of every saved revision	The student only, until submitted
Submitted worksheet	The exact revision the student submitted, with the AI use note and the preserved first attempt, and the facilitator's feedback on it	The student and the facilitators of that cohort. Team members share venture evidence but each keeps their own worksheets

Record	Content	Who can see it in the application
Venture record	The venture's direction, claims, findings with the five permissions recorded for each source, decisions and changes of direction	The venture's members and the cohort's facilitators
Audit	Who prepared, accepted, revoked, released or paused what, and when; review outcomes in sequence	Not shown in any screen. Written by the application; read by the Foundiro operator in the database

Students can export their venture record. The AI task briefing is text the student copies into an assistant of their own; the workspace does not call any AI service and holds no AI provider key.

When a worksheet question is retired from a lesson, answers already saved under it are not deleted: they are carried forward unchanged with every later save, stay in each revision snapshot, submission and export, and are shown to the student read-only as earlier answers kept on record.

Access and security measures

- Sessions last eight hours and use HttpOnly, Secure, SameSite=Strict cookies.
- Invitation and reset codes are single use, hashed in storage, expire after about three days, and can be revoked and reissued. Sharing is in person; nothing is emailed.
- Password changes and recovery rotate the recovery code and end other sessions.
- Failed sign-ins are rate limited: a per-account budget and a site-wide circuit breaker, both expiring after fifteen minutes. A successful sign-in clears that account's failed-attempt count. It does not clear the site-wide count, which expires on its own.
- Accounts are paused, not deleted; their records are retained for audit. A cohort can be paused as a whole.
- Facilitator and operator routes are scoped on the server; a facilitator cannot read another cohort, and an institution cannot read another institution.

What reaches an AI briefing

- Fields marked private (for example the rehearsal reflection) are never placed in a briefing, including when a student selects every field.
- The student's conclusion, decision criterion and reflection are never drafted by the AI; the return format puts critique of them under suggestions only.
- The earliest recorded decision criterion of a connected worksheet is included in the briefing as context, with its revision and date, so that the assistant cannot invent a threshold and so that a late-written criterion is visible as such. It is read, not written.
- Research, consent and ledger fields are kept out of the briefing unless the student selects them explicitly, and only sources whose owners permitted AI analysis are included.
- The student's private lesson record (notes, highlights, practice answers) is not part of any briefing.

How lessons open in guided progression

In a cohort set to guided progression, a student sees the first lesson; each next lesson opens for that student in that venture when a facilitator continues the student's current submission. Feedback marked revise opens nothing. Two exceptions exist, both written to the audit:

- A cohort facilitator may release lessons up to a chosen one, for one student or for the whole cohort, with a written reason. The record says release, never continue, and it is not an approval of any work.
- When the operator switches a cohort from open to guided, every lesson a person had already saved work in stays open, recorded as preserved, so nothing is taken away.

Open lessons never close. Staff are never gated: a facilitator can preview any lesson without writing anything.

What has been confirmed, and how

Three kinds of evidence are distinguished: automated tests on an isolated database with fictional data (local), calls to the hosted service's application routes with a fictional cohort (live API), and a person working through the hosted screens in a browser with fictional people (browser).

Statement	Evidence	Date
The workspace is hosted at the Foundiro domain with a hosted PostgreSQL database, built from a reviewed source archive published manually, with no AI agent involved	Byte comparison of the served build against the reviewed files (live)	11 November 2026
Invitation-only access, single-use codes, cookie flags, rate limits, cross-institution denial and the learner, staff and operator boundaries	Automated tests (local); invitation, sign-in and scope checks against the hosted routes (live API)	11 November 2026
Private fields never reach a briefing; the worksheet's first attempt is preserved; feedback reaches the student	Automated tests with sentinel values (local); a fictional student and facilitator journey on the hosted service (browser)	11 November 2026

Statement	Evidence	Date
Guided progression: no submission before the practice is saved; the next lesson opens only on the facilitator's continue; release and preservation are audited; concurrent continue and resubmit cannot leave inconsistent state	Automated tests on an isolated real PostgreSQL instance, two runs, no deadlocks (local); a bounded fictional guided cohort on the hosted service (live API)	11 November 2026
Answers under a retired worksheet question survive read, save, resubmission, history and export	Automated test (local), added in the second correction pass	11 November 2026
A successful sign-in clears the account's failed-attempt count and not the site-wide count	Automated test (local), added in the second correction pass	11 November 2026
A full production snapshot (19 tables) can be restored into an isolated database and compared row by row	Restore into an isolated in-memory database; production untouched (local)	11 November 2026
The hosting provider's point-in-time recovery is enabled for the database	Observation in the provider's console	11 November 2026
The owner's operator account can sign in and reach programme administration	Independent review observed the sign-in and the administration screen (browser)	11 November 2026

What has not been confirmed

- Restoration of a backup onto a separate full PostgreSQL service as a disaster-recovery rehearsal. Only the isolated snapshot comparison above has been done.
- The hosting region, the provider's data-processing terms, and whether they satisfy the university's data-protection requirements. These are to be confirmed with the university before any real student is enrolled.
- A data-retention and withdrawal procedure for a student who leaves the programme. Today accounts are paused and records retained; deletion on request has no application route and would be done by Foundiro in the database directly.

- Accessibility of the workspace and the PDFs against a formal standard. No PDF/UA or WCAG certification is claimed.
- Every one of the 84 lessons opened individually in a browser on the hosted service. The lesson content is checked automatically; the browser journey covered a sample.
- Behaviour of any external AI assistant. The workspace prepares text; what an assistant does with it is outside the workspace.
- Classroom use with real students. Every test so far used fictional people and fictional ventures.

Operations

Activity	Who	How
Create an institution, cohort and facilitator accounts	Foundiro operator	In the workspace's programme administration
Enrol students and prepare invitations	The cohort's facilitator	In the workspace; codes shared in person
Switch a cohort between guided and open progression	Foundiro operator, at the institution's request	One setting per cohort; nothing is removed when switching
Release lessons ahead of the normal sequence	The cohort's facilitator, with a written reason	In the workspace; audited; shown as a release, not an approval
Pause a person or a cohort	Facilitator (own cohort) or operator	Records retained
Reset a lost password	Operator prepares a reset code after the institution confirms identity; the person also has their own recovery code	Shared in person
Read the audit trail or act on records outside the application	Foundiro operator	In the database, under the agreement with the institution; the application has no screen for it
Software changes	Foundiro, after independent review and tests	Published manually; the institution is told before a change that affects its cohorts

What to agree with the university before enrolment

1. Which cohorts use the workspace and which run on paper
2. The university's data-protection assessment, including the hosting questions above
3. Who at the university holds the facilitator and reviewer accounts
4. Whether cohorts run guided or open progression, and who may release lessons ahead of sequence
5. The approved AI services for students, or the decision that none are used

6. The retention period for student records after the programme and the route for a withdrawal request

This note describes the state on 11 November 2026 and is updated with each change to the workspace. Statements in the "not confirmed" list are limits, not plans; none should be read as a promise.