04 - Institution Admin Guide

How institution administrators manage setup, users, classes, subjects, teacher assignments, guardian links, reports, final results, and governance.

Use this guide for testing, pilot, and early user onboarding. Screens may change while OTE Learn is being improved. If a menu item is missing, your role may not have permission to use it.

Contents

1 Admin role overview
2 Institution setup checklist
3 Managing classes and subjects
4 Managing learners and placements
5 Managing teachers
6 Managing guardians
7 Academic periods and reports
8 Security and privacy admin checks

1. Admin role overview

Institution admins configure the operational structure of the LMS. This includes institution settings, classes, subjects, teacher assignments, learner placement, academic periods, guardian links, reports, and access reviews.

- Do setup before testing with learners.
- Use test users first.
- Review access often.
- Keep institution data accurate.
- Remove users who no longer belong to the institution.

2. Institution setup checklist

1. Confirm institution name, email, phone, address, status, and branding.
2. Create grade/programme structure.
3. Create classes for the correct academic year.
4. Create subjects.
5. Assign subjects to classes.
6. Assign teachers to class subjects with correct permissions.
7. Place learners into the correct class.
8. Create academic periods such as terms or semesters.
9. Configure assessments and report distribution rules.
10. Link guardians only after confirming authority.

Do not let setup users rely on current_institution_id alone as admin proof. Access should come from approved roles and permissions.

3. Managing classes and subjects

- Use clear class names such as Grade 8A 2026.
- Keep academic year consistent across class, learner placement, assessment allocations, and reports.
- Disable subjects when no longer used instead of deleting historical records.
- Duplicate classes carefully when rolling to a new academic year.
- Check teacher assignments after duplication.

4. Managing learners and placements

Learners should belong to the correct institution and class for the academic year. Wrong placement can hide subjects or show the wrong assessments.

1. Search learner by name or email.
2. Confirm the correct academic year.
3. Place the learner in the correct class.
4. Confirm the learner sees the correct subjects.
5. If the learner moves class, end or update placement according to your process.

If reports are blank, check academic year, academic period dates, class placement, result release, counts-towards-report flags, and report distribution percentages.

5. Managing teachers

- Assign teachers to class subjects.
- Set whether they can create assessments.
- Set whether they can mark assessments.
- Set whether they can view results.
- Use primary teacher only where needed.
- End assignments when the teacher no longer teaches that class or subject.

6. Managing guardians

1. Open Student Guardians.
2. Select academic year and grade.
3. Click Load learners.
4. Select the learner.
5. Add guardian name, email, relationship, and access flags.
6. Send invite.
7. Guardian must sign in with the same email.
8. Review and remove guardian access when necessary.

- A guardian can be linked to more than one learner.
- A learner can have more than one guardian.
- Guardian access should usually continue across years unless removed.
- Disputes about guardianship must be handled by the institution.

7. Academic periods and reports

- Create the academic year periods before generating reports.
- Make sure period dates cover the assessment due dates.
- Use Counts towards report on assessment allocations that must count.
- Set report distribution percentages to exactly 100 percent per subject.
- Use Must pass only where institution policy requires it.
- Final transcripts should be generated only after all periods are finalised.

8. Security and privacy admin checks

- Test student direct links to admin pages and confirm they are blocked.
- Check that teachers see only assigned classes and subjects.
- Check guardian access with a test guardian account.
- Rotate exposed secrets immediately if pasted into chat, email, screenshots, or source.

- Review support tickets and feedback for privacy risks.
- Keep public documentation, Privacy, and Terms links visible.