Spelling Mastery — School Compliance Pack

Access Control and Identity Management Policy

Document owner: [Company Name] Version: 1.0 Last updated: [YYYY-MM-DD]

1. Purpose

Defines identity and access requirements to protect school and student data.

2. Principles

- Least privilege
- Need-to-know access
- Separation of duties for privileged actions
- Timely joiner/mover/leaver processing
- Periodic access recertification

3. User Roles

Typical roles:

- Student user
- Teacher/admin user
- School admin
- Platform support/admin

Role entitlements must be documented and approved.

4. Authentication Requirements

- Strong password requirements for privileged users
- Session/token validation for protected operations
- Optional/enforced MFA for administrator-level access
- Account lockout/rate limiting for repeated failed attempts

5. Provisioning and Deprovisioning

- Access granted only with approved request.
- Access removed promptly when no longer needed.

- Privileged access requires additional approval and logging.

6. Access Reviews

- Periodic review (at least quarterly) of privileged accounts.
- Removal or correction of excessive/stale permissions.
- Review evidence retained for audit.

7. Logging and Monitoring

- Log sensitive account and privilege changes.
- Monitor for anomalous access patterns.
- Escalate suspected misuse under incident procedures.

8. Exceptions

Any policy exception must:

- be documented,
- include risk acceptance owner,
- include expiry date and compensating controls.