SOPs - Use of Turnitin Similarity Detection Software

These SOPs establish standardized protocols for the responsible use of Turnitin Similarity Detection Software under the Higher Education Commission (HEC) framework. They aim to prevent misuse, ensure compliance with HEC policies, and safeguard academic and research integrity across all participating institutions.

These SOPs apply to:

- Institutional Administrators
- Instructor Accounts
- Student Accounts

Roles & Responsibilities

Institutional Administrators

- Create, manage, suspend, and deactivate user accounts in accordance with these SOPs.
- Ensure correct role assignment (Instructor vs. Student).
- Maintain accurate and updated user records.
- Monitor account usage at the institutional level.
- Act immediately upon detection or suspicion of misuse.
- Cooperate fully with HEC during audits, reviews, and investigations.

Instructors

- Use Turnitin exclusively for institutional academic and research purposes.
- Ensure submissions belong to enrolled students or supervised research.
- Maintain confidentiality of login credentials.
- Refrain from sharing access with students, colleagues, or third parties.

Students

- Access Turnitin only through officially assigned Student accounts.
- Submit only their own academic work related to enrolled courses or research.
- Never use Instructor accounts under any circumstances.

Account Creation & Role Assignment

Instructor Accounts

- Issued only to permanent or contract faculty members.
- Verification through official institutional email is mandatory.
- Only one Instructor account per individual is permitted.
- Accounts must be deactivated prior to faculty clearance in case of disaffiliation (to be reflected in NDC records).
- Re-issuance of accounts to previously suspended users requires prior HEC approval.

Student Accounts

- Issued for a defined academic timeframe only.
- Access must be revoked upon course completion, graduation, or withdrawal.
- Sharing of Instructor credentials with students is strictly prohibited.

Account Approval & Record Maintenance

Institutions shall maintain a secure log containing:

- User name
- Role assigned
- CNIC / Employee ID / Registration No.
- Official institutional email
- Date of account creation
- Date of deactivation (where applicable)

Account Usage Protocols

Institutional Custodianship

- The Vice Chancellor / Head of Institution shall ensure the responsible use of Turnitin in full compliance with HEC policy.
- A formally notified Turnitin Administrator shall be responsible and accountable for secure management of the account.
- In the event of a change in the Turnitin Administrator, the HEI shall formally notify the newly appointed administrator and inform HEC accordingly.
- The administrator account shall be used exclusively by the notified individual; any violation shall result in permanent suspension of the institutional account.

Authorized Academic Use

Turnitin access shall be utilized exclusively for institutional academic and research purposes, including:

- Theses and dissertations
- Research manuscripts
- Assignments of duly enrolled students
- Academic supervision and evaluation (e.g., plagiarism checking to support research guidance, assessment of originality, feedback on scholarly writing, and quality assurance in teaching and learning processes)

All submissions must originate from enrolled students or HEI faculty and must be directly related to assigned courses or formally approved research supervision. Usage is strictly confined to academic and research work conducted within the institution.

Prohibited Use:

- Submissions on behalf of third parties, foreign institutions, or commercial entities.
- Paid plagiarism or AI-detection services.
- Automated or bot-like submission behavior.
- Credential sharing with external users.

Monitoring & Compliance

- Administrators shall quarterly review submission activity.
- Periodic reconciliation of active users is mandatory.
- Irregular or excessive activity shall be investigated.
- Suspected misuse requires immediate suspension and reporting to HEC.

Disciplinary Proceedings

Offense Level	User Category	Description	Penalty
Minor	Instructor	Limited misuse due to negligence	Warning, mandatory training, temporary suspension
Major	Instructor	Repeated misuse, account sharing, third-party/commercial use	Permanent access termination, disciplinary proceedings
Severe	Administrator / Instructor	Issuing Instructor accounts to students/non-HEI personnel, organized misuse, repeat violations	Termination of institutional account; disciplinary action under statutes

Suspension & Reinstatement

- Immediate Action: Temporary suspension of the account, documentation of findings, and notification to UAPSC.
- Case Evaluation: UAPSC shall evaluate cases in accordance with the Anti-Plagiarism Policy and established Academic Integrity practices, and conclude the case within 30 days.
- Reporting: Findings of the committee shall be communicated to HEC immediately.

- Reinstatement Conditions: Written justification, signed acknowledgment of the Acceptable Use Policy, completion of an awareness session, and final approval from HEC.
- Repeat Offenders: Permanent suspension of the account, formal notification to the institution, and no re-issuance of accounts.

Prevention of Commercial Misuse

- Institutions shall prohibit use of Turnitin for commercial purposes.
- Quarterly audits must be conducted to identify third-party linkages.
- Evidence of commercial exploitation shall be reported to HEC immediately.

Awareness & Capacity Building

- Biannual awareness sessions conducted jointly by Turnitin and HEC for Institutional Administrators and Instructors (mandatory attendance).
- Annual awareness sessions at HEI level for all instructors, conducted by Institutional Administrators. Topics include:
  - Acceptable Use Policy
  - Consequences of misuse
  - Ethical use of similarity detection tools

User Declarations

All instructors shall sign an annual declaration confirming compliance with these SOPs.

Reporting & Escalation

- Institutions shall submit quarterly compliance reports to HEC.
- Immediate incident reporting is required in case of suspected misuse.
- HEC shall maintain a centralized misuse tracking record.