

TSUULL Data Collection Policy

1. Purpose

This Data Collection Policy establishes the principles and requirements governing the collection, use, storage, protection, retention, sharing, and disposal of personal and institutional data by Tashkent State University of Uzbek Language and Literature (TSUULL).

The purpose of this Policy is to ensure that data is collected lawfully, fairly, transparently, securely, and only for legitimate academic, administrative, research, and institutional purposes.

2. Scope

This Policy applies to:

- students, applicants, graduates, and prospective students;
- academic and administrative staff;
- researchers, visiting scholars, and other university personnel;
- contractors, partners, and service providers processing data on behalf of TSUULL;
- university websites, online platforms, applications, information systems, and other digital services;
- data collected in physical or electronic form.

This Policy applies to personal data and, where appropriate, institutional, academic, research, financial, and operational data collected or processed by TSUULL.

3. Definitions

Personal Data means information relating to an identified or identifiable individual.

Data Subject means an individual whose personal data is collected or processed.

Data Collection means obtaining, recording, receiving, or otherwise acquiring data from individuals, systems, documents, or other lawful sources.

Processing includes collecting, storing, organizing, using, modifying, transferring, sharing, archiving, and deleting data.

Sensitive Personal Data means categories of personal information requiring enhanced protection under applicable legislation and university requirements.

Third Party means an external individual, organization, institution, or service provider that is not the data subject or TSUULL.

4. Principles of Data Collection

TSUULL shall collect and process data according to the following principles:

4.1 Lawfulness and Transparency

Data shall be collected and processed in accordance with applicable legislation, contractual obligations, university regulations, and other lawful bases.

Where appropriate, individuals shall be informed about what data is being collected, why it is needed, how it will be used, how long it may be retained, and with whom it may be shared.

4.2 Purpose Limitation

TSUULL shall collect data for specified, explicit, and legitimate purposes. Data shall not be subsequently used for purposes incompatible with the purpose for which it was originally collected, unless permitted by applicable law or with appropriate authorization.

4.3 Data Minimization

Only data that is reasonably necessary for a legitimate university purpose shall be collected.

University departments shall avoid collecting excessive, irrelevant, or unnecessary personal information.

4.4 Accuracy

Reasonable measures shall be taken to ensure that collected data is accurate, complete, and kept up to date when necessary.

Individuals may be provided with appropriate mechanisms to request correction of inaccurate personal data.

4.5 Security and Confidentiality

TSUULL shall implement appropriate administrative, technical, and physical safeguards to protect data against unauthorized access, disclosure, alteration, loss, destruction, or other unlawful processing.

Access to personal and confidential data shall be limited to authorized individuals who require it for legitimate university duties.

4.6 Accountability

Departments and employees responsible for collecting or processing data shall be accountable for complying with this Policy and applicable legal requirements.

5. Categories of Data That May Be Collected

Depending on the purpose, TSUULL may collect the following categories of information:

5.1 Student and Applicant Data

- name and contact information;
- date and place of birth;
- identification or passport information where legally required;
- admission and enrollment information;
- academic records and grades;
- attendance and academic progress;
- scholarship and student-support information;
- university account and identification information;
- information necessary for examinations and assessments.

5.2 Staff and Employment Data

- identification and contact information;
- employment and professional records;

- qualifications and academic credentials;
- payroll and administrative information;
- performance and training records;
- information required to comply with employment and legal obligations.

5.3 Research Data

Research-related data may include participant information, survey responses, interview data, academic research records, and other information necessary for approved research activities.

Research involving personal or sensitive data shall comply with applicable ethical, legal, and institutional requirements.

5.4 Website and Digital-Service Data

TSUULL may collect information generated through its websites and digital services, including:

- account information;
- login and authentication data;
- device and browser information;
- IP addresses and technical logs;
- information submitted through online forms;
- system usage and security information.

Where cookies or similar technologies are used, TSUULL should provide appropriate notice and obtain consent where required by applicable law.

6. Sources of Data

Data may be collected directly from individuals through:

- admission and enrollment forms;
- employment applications and personnel procedures;
- university registration systems;
- surveys and questionnaires;
- research activities;
- examinations and assessments;
- university websites and applications;
- official correspondence and communications.

Where lawful and necessary, TSUULL may also obtain information from authorized third parties, government institutions, educational organizations, accreditation bodies, service providers, or other legitimate sources.

7. Consent

Where consent is the appropriate legal basis for collection or processing, TSUULL shall obtain consent in a manner that is informed, specific, and appropriately documented.

Consent shall not be assumed merely because an individual provides information, unless the applicable legal framework establishes another lawful basis. Where consent is relied upon, individuals should be informed of how they may withdraw consent, subject to legal and contractual limitations.

8. Collection of Sensitive Data

TSUULL shall apply enhanced safeguards when collecting or processing sensitive personal data.

Sensitive information shall only be collected when there is a legitimate and lawful university purpose and when the collection is permitted by applicable legislation.

Access to such information shall be restricted to authorized personnel with a genuine need to access it.

9. Use of Collected Data

Collected data may be used for legitimate purposes including:

- admission, enrollment, and student administration;
- teaching, learning, and assessment;
- academic advising and student support;
- employment and human-resource administration;
- research and scholarly activities;
- examination administration;
- financial and accounting activities;
- library and information services;
- university security and access management;
- information technology and cybersecurity;
- communication with students, staff, applicants, and graduates;
- legal, regulatory, accreditation, and reporting obligations;
- institutional planning, quality assurance, and statistical analysis.

TSUULL shall not use personal data for unrelated purposes without an appropriate lawful basis.

10. Data Sharing and Disclosure

Personal data may be shared internally only with authorized university personnel who require the information to perform their responsibilities.

TSUULL may disclose data to external parties when:

- required or permitted by law;
- necessary to provide an authorized university service;
- required for legitimate academic or research activities;
- necessary to protect the rights, safety, or security of individuals or the university;
- authorized by the relevant data subject where consent is required;
- necessary to meet contractual, regulatory, accreditation, or governmental obligations.

Third parties processing personal data on behalf of TSUULL should be subject to appropriate contractual, confidentiality, and security requirements.

11. Data Retention

TSUULL shall retain data only for as long as necessary to fulfill the purpose for which it was collected or to satisfy applicable legal, regulatory, academic, financial, archival, or institutional requirements.

Retention periods should be established by the responsible university departments in accordance with applicable records-management requirements.

When data is no longer required, it shall be securely deleted, destroyed, anonymized, or otherwise disposed of in accordance with university procedures.

12. Data Security

TSUULL shall use reasonable safeguards appropriate to the nature and sensitivity of the data.

Security measures may include:

- role-based access controls;
- authentication and password controls;
- encryption where appropriate;
- secure data storage;
- backup and recovery procedures;
- network and endpoint security;
- staff confidentiality obligations;
- security awareness and training;
- monitoring and logging;
- secure disposal of records.

Employees and other authorized users shall not access, copy, disclose, or use university data for unauthorized purposes.

13. Data Breach and Security Incidents

Any suspected or confirmed unauthorized access, loss, disclosure, alteration, destruction, or other compromise of personal or confidential data shall be reported promptly through the university's designated incident-reporting procedures.

TSUULL shall assess reported incidents and, where required, take appropriate containment, investigation, remediation, documentation, and notification measures in accordance with applicable law and university procedures.

14. Rights of Data Subjects

Subject to applicable legislation and legitimate university requirements, individuals may have rights concerning their personal data, including the right to:

- receive information about the collection and use of their data;
- request access to personal data held about them;
- request correction of inaccurate or incomplete data;
- request deletion or restriction of processing where legally applicable;
- object to certain processing activities where legally applicable;
- withdraw consent where processing is based on consent;
- submit a complaint regarding the handling of their personal data.

Requests shall be handled through procedures established by TSUULL and applicable law.

15. Responsibilities

15.1 University Administration

University leadership shall support appropriate governance, resources, and oversight for data protection and responsible data management.

15.2 Departments and Faculties

Departments and faculties shall:

- collect only necessary data;
- ensure that collection has a legitimate purpose;
- maintain appropriate records;
- restrict access to authorized personnel;
- report suspected data incidents;
- comply with university data-management procedures.

15.3 Employees and Other Users

Individuals with access to TSUULL data shall:

- use data only for authorized purposes;
- maintain confidentiality;
- protect credentials and access mechanisms;
- follow university security procedures;
- avoid unauthorized disclosure or copying;
- promptly report suspected security incidents.

15.4 Third-Party Service Providers

Service providers processing TSUULL data shall comply with applicable contractual, security, confidentiality, and data-protection requirements.

16. Data Quality and Review

University departments shall periodically review the data they collect to determine whether it remains necessary, accurate, relevant, and proportionate to the stated purpose.

New data-collection activities, particularly those involving sensitive or large-scale personal data, should undergo appropriate institutional and legal review before implementation.

17. International and Third-Party Transfers

Where personal data is transferred to another country or to an external organization, TSUULL shall ensure that the transfer is carried out in accordance with applicable legal requirements and appropriate safeguards.

Contracts, confidentiality requirements, security controls, and other protective measures shall be used where appropriate.

18. Transparency and Notices

Where personal data is collected directly from individuals, TSUULL should provide an appropriate privacy notice explaining, where applicable:

1. the identity of the organization collecting the data;
2. the categories of data collected;
3. the purpose of collection;
4. the applicable legal basis;
5. intended recipients or categories of recipients;
6. retention or applicable retention criteria;
7. relevant data-subject rights;
8. how individuals can contact the university regarding their data.

19. Policy Compliance

Failure to comply with this Policy may result in corrective or disciplinary action in accordance with TSUULL regulations, employment rules, contractual terms, and applicable legislation.

Violations involving unauthorized access, disclosure, alteration, destruction, or misuse of university data may also be subject to legal consequences.

20. Policy Review and Amendment

This Policy shall be reviewed periodically and whenever significant changes occur in applicable legislation, university operations, information systems, or data-processing practices.

TSUULL may amend this Policy when necessary to improve data protection, address emerging risks, or maintain compliance with applicable requirements.

21. Contact and Complaints

Questions, requests, or complaints concerning the collection or processing of personal data should be submitted through the official TSUULL administrative or data-protection contact designated for this purpose.

TSUULL shall maintain appropriate procedures for receiving, reviewing, documenting, and responding to such requests.

22. Final Provisions

This Policy establishes the general framework for responsible data collection at TSUULL. It should be implemented together with applicable legislation of the Republic of Uzbekistan, TSUULL's internal regulations, information-security requirements, records-management procedures, research-ethics requirements, and other relevant institutional policies.

Where a conflict exists between this Policy and a mandatory legal requirement, the applicable legal requirement shall prevail.