Kingdom of Saudi Arabia
Ministry of Education
University of Tabuk
Data Management Office

المملكة العربية السعودية
وزارة التعليم
جامعة تبوك
مكتب وحدة حوكمة البيانات

Personal Data Privacy Policy

Document Specifications

Document Title	Personal Data Privacy Policy
Institution	Tabuk University
Document Owner	Data Management Office
issue Number	1.0
Status	issued
issue Date	11 January 2024
Document Classification	internal

Modifications

Issue	Date	Modifications	Edit	Review	Approval
1.0	11 January 2024	None	Dr. Mariam Al-Shihry	Dr. Mohammed Al-Otaibi	Digital Transformation Committee

Approvals

Name	Position	Date	Signature
Dr. Mohammed Mutaib Al-Otaibi	Director of Data Management Office	11 January 2024	
Members of Digital Transformation Committee	Standing Committee for Digital Transformation	15 February 2024	Meeting minute

Glossary

Term	Definition
The University	University of Tabuk
Business Directories	Agencies, Deanships, Units, Directorates, Departments
Data	Unprocessed set of facts, such as numbers, letters, still images, video, audio recordings, or emojis
Personal Data	Any statement—regardless of its source or form—that can lead to the identification of an individual, either directly or indirectly when combined with other data. This includes, but is not limited to, names, personal identification numbers, addresses, contact numbers, bank account and credit card numbers, health data, still or moving images of the user, and other personal or special-characteristic data from which a specific individual can be identified.
Accessing Data	Logical and Physical access to the university's data and technical resources for the purpose of using them.
Data Subject	Person to whom the personal data relates, or their representative, or the person who has legal guardianship over them
Personal Data Processing	All operations carried out on personal data by any means, whether manual or automated. These operations include, but are not limited to, collecting, transferring, saving, storing, sharing, destroying, analyzing, extracting patterns, drawing conclusions, and linking with other data.
Personal Data Disclaimer	Enabling any person—other than the University's Data Management Office—to obtain, use, view, or access personal data by any means and for any purpose.
Personal Data Breach	Disclosure of personal data, obtaining it, or enabling access to it without authorization or legal basis, whether intentionally or unintentionally
Destruction of Personal Data	Any action that results in the removal of personal data, making it impossible to access or recover, including erasure or deletion, whether electronic or physical.
Privacy Notice	An external statement addressed to individuals that explains the content of personal data, the methods of its collection, the purpose of its processing, how it will be used, the relevant parties with whom the data will be shared, the retention period, and the method of disposal
Data Classification Levels	Highly Confidential, Confidential, Restricted, Public

Error! Bookmark not defined.

1.1 4**1.2** 4**1.3** 4**1.4**4**1.5** 42.
Policy Clauses 8

2.1 Error! Bookmark not defined.2.2 5**2.3**6**2.4** 6**2.5**
83. Related Documents 12

1.Introduction

1.1 Purpose of the Document

In response to the controls of the National Data Management Office and the relevant standards requiring the establishment of data governance policies within governmental entities, and based on the national data governance policies that have been developed, the University's Data Office has developed a Personal Data Protection Policy in alignment with the policies of the National Data Management Office.

The purpose of this policy is to demonstrate the University's commitment to protecting the privacy of beneficiaries' personal data. This policy aims to establish the fundamental rules for safeguarding personal data that is processed and must be followed by the University's business departments to ensure the security of personal data for users.

1.2 Policy Coverage and Application

This policy applies to all University entities that directly or indirectly handle personal data of all University members (faculty, staff, students) and others who have a contractual or statutory relationship with the University. The provisions of this policy do not apply in the following cases:

- To fulfill legal requirements under applicable laws, regulations, and policies.
- To meet judicial requirements.
- To fulfill obligations under agreements to which the Kingdom is a party.
- To protect health, public safety, or the vital interests of individuals.

1.3 Policy Review Schedule

This policy should be reviewed regularly, at least once annually, according to the guidance of the policy's overall supervisor.

1.4 Compliance Monitoring

Compliance with the Personal Data Protection Policy is measured according to the standards and performance indicators set by the University's Data Management Office, in alignment with the requirements of the National Data Management Office. Compliance standards are periodically reviewed by the Director of the Data Management Office.

1.5 Roles and Responsibilities Matrix

Supervisory Committee	Responsible for approving the policy and plans, and making decisions to resolve issues and handle escalation cases.
Data Governance Unit Office	The Data Governance Unit Office is the entity responsible for preparing the University's Personal Data Protection Policy and related procedures in alignment with the directives of the National Data Management Office, including: • Preparing and updating the Personal Data Protection Policy. • Preparing, updating, and approving the Privacy Notice for use by business departments that handle personal data. • Supervising the identification of personal data handled by the University in collaboration with business departments. • Approving the plan and mechanism for implementing the Personal Data Protection Policy. • Preparing compliance reports regarding the University's Personal Data Protection Policy for stakeholders. • Developing awareness programs to raise knowledge and promote a culture of personal data protection. • Reviewing requests for data sharing submitted by various entities, directing them to business data representatives, and verifying that the requested data is properly classified.
Business Directories	Implementation of the Personal Data Protection Policy through: • Collaborating with the Data Management Office to identify the reference sources of personal data within the University.

	• Complying with the Personal Data Protection Policy and Privacy Notices.
Strategy Sector (Deanship of Development and Quality)	Responsible for reviewing and updating contracts, service level agreements, and operational agreements in accordance with the privacy policies and procedures approved by the entity's senior management.
Deanship of Information Technology	The IT departments are responsible for implementing the policy provisions across all systems and databases.
Cybersecurity Department	Responsible for identifying, documenting, and approving cybersecurity requirements related to the protection of personal data, in alignment with the directives of the National Cybersecurity Authority. This includes: • Monitoring and auditing the implementation of protection controls on personal data. • Preparing reports for stakeholders and managing escalations regarding the application of protection controls on personal data, and sharing these reports with the Data Management Office.
Risk Management	Responsible for assessing the risks and potential impacts of personal data processing activities, determining the acceptable level of risk, approving it at the University level, and sharing the assessment results with the Municipal Data Office and sector stakeholders.
Legal Department	Responsible for providing consultations regarding notices or issues related to personal data breaches, reviewing the legal wording of privacy notices and contracts, and advising on data subjects' rights