

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



المملكة العربية السعودية
وزارة التعليم
جامعة تبوك
مكتب وحدة حوكمة البيانات

Freedom of Information Policy at the University of Tabuk

V.1.0



Document Details

Document Name	Freedom of Information Policy
Institution	University of Tabuk
Document Owner	Data Governance Unit Office
Version Number	1.0
Status	Issued
Version Date	January 20, 2024
Document Classification	Internal

Modifications Date

S	Date	Modifications	Release	Review	Approval
1.0	January 20, 2024	None	Dr. Mariam Al-Shahry	Dr. Mohammed Al-Otaibi	Standing Committee for Digital Transformation

Approvals

Name:	Position	Date	Signature
Dr. Mohammed Mutaib Al-Otaibi	Director of the Data Management Office	January 22, 2024	
Standing executive committee for digital transformation	Standing Committee for Digital Transformation	February 15, 2024	



Definition Table

Term	Definition
University	University of Tabuk
Business Administrations	Vice rectors, Deanships, Units, Departments, and Divisions.
Data	A collection of facts in their initial or unstructured form, such as: numbers, letters, static images, video, audio recordings, or emojis.
Data Confidentiality	Maintaining authorized restrictions on access to or disclosure of data.
Authentication	Verifying the identity of any user, process, or device as a prerequisite for allowing access to technical resources.
Data Access	The ability to logically and physically access the University's data and technical resources for the purpose of utilization.
Public Information	Processed, non-protected data received, produced, or handled by the university, regardless of its source, form, or nature.
Applicant	Any entity from the public, private, or third sector, or any individual submitting a request for data sharing.
Data Sharing Request	A designated form used to request data sharing, which includes information about the applicant, the requested data, and the purpose for which data sharing is requested.
Data Classification Levels	Data classification levels are: highly confidential, confidential, restricted, and public.



1. Introduction

1.1 Purpose of the Document

In response to the initiative of the National Data Management Office (NDMO) and related initiatives that mandate the establishment of data governance policies within government entities—based on the developed national data governance policies—the Data Office at the University has developed the Freedom of Information Policy document, in alignment with the policies of the National Data Management Office in the Kingdom.

1.2 Scope and Application of the Policy

This policy applies to all individual requests for access to or acquisition of information classified as public and owned by the University.

The policy does not apply to data classified as highly confidential, confidential, or restricted.

1.3 Policy Review Schedule

This policy must be reviewed regularly, at least once annually, as directed by the General Supervisor of the Policy and as requested by the University's Data Management Office.

1.4 Compliance Monitoring

Compliance with the Freedom of Information Policy shall be measured according to the performance standards and indicators established by the University's Data Management Office and in accordance with the requirements of the National Data Management Office.

Compliance standards are to be reviewed periodically by the Director of the Data Management Office.



1.5 Roles and Responsibilities

Role	Responsibility
Steering Committee	Reviews compliance reports and makes decisions and corrective actions to resolve issues and escalation cases.
Data Governance Unit Office	The Data Governance Unit Office is responsible for preparing and implementing policies and procedures related to exercising the right of access to or obtaining public information. This includes: - - Preparing and updating the freedom of information policy. - Preparing and documenting the procedures for processing requests to access public information. - Preparing and documenting policies and procedures for retaining and disposing of request records in accordance with the regulations and legislations related to the university's businesses and activities. - Preparing and documenting the necessary procedures for managing, processing, and documenting extension requests and rejected requests, defining the roles and responsibilities of the specialized working team, and identifying the cases in which the regulatory body and the office must be notified according to the administrative hierarchy and within the specified timeframe for processing requests. - Ensuring that individuals are properly notified in cases where the request is fully or partially denied, clarifying the reasons for rejection, and informing them of their right to appeal and how to utilize this right within a period not exceeding fifteen (15) days from the date of the decision. - Developing awareness programs to promote a culture of transparency and enhancing understanding of the approved freedom of information policies and procedures. - Reviewing requests for access to public information and directing them to business data representatives after ensuring that the requested data is classified as public. - Periodically monitoring compliance with freedom of information policies and procedures.



	- Setting the necessary criteria to determine the fees associated with processing requests for access to or obtaining public information, based on the nature and volume of the data, the effort involved, and the time spent—in accordance with the data monetization policy—and documenting all records of access to information requests and the decisions taken regarding them, provided that these records are reviewed to address cases of misuse or non-responsiveness.
Business Administrations	Business Administrations study and process requests for access to public information, which includes: - Studying the requests and verifying their fulfillment of statutory requirements. - Executing the requests in compliance with the policy and controls. - Participating in defining the key data produced by the Administration.
Deanship of Information Technology	The Deanship of Information Technology is responsible for providing secure digital channels for requesting information (public information request forms), including: - Verifying the identity of individuals before granting them the right to view or obtain public information, in accordance with controls approved by the National Cybersecurity Authority and related entities. - Automating requests and verifying the application of all controls, standards, and service level agreements. - Providing available digital data to enable business administrations to process the requests.
Cybersecurity Administration	Ensuring alignment with the policies and controls issued by the National Cybersecurity Authority.
Risk Management Administration	Reviewing reports on compliance with the policy implementation and defining risks of non-compliance.

2. The Main Principles of Freedom of Information

First Principle: Transparency

The applicant has the right to know information related to the university's public activities, in order to promote integrity, transparency, and accountability—unless such information is protected and not permitted to be disclosed.

Second Principle: Necessity and Proportionality

The applicant has the right to receive a clear and explicit justification in cases where the



university imposes any restrictions on the disclosure of information, if the requested information is protected or not authorized for disclosure.

Third Principle: Disclosure Is the Default for Public Information

The applicant has the right to view public university information that is *not protected*. The applicant is not required to have a specific status or a particular interest in this information to obtain it, nor will they be face any legal accountability related to this right.

Fourth Principle: Equality

All requests to view or obtain public information shall be dealt with on the basis of equality and non-discrimination between individuals.

3. Individual Rights Regarding Access to or Obtaining Public Information

Firstly: The right to view or obtain any **non-protected public information** held by the University.

Secondly: The right to **know the reason for the refusal** to view or obtain the requested information.

Thirdly: The right to appeal decisions that reject requests to access or obtain the requested information.

4. Main Steps for Accessing or Obtaining Information

Main Requirements for Requests to Access or Obtain Public Information:

1. The request must be in written or electronic form.
2. The “Public Information Request Form” approved by the university must be completed.
3. The request must be for the purpose of accessing or obtaining public information.
4. The request form must include details on how the final decision and notifications will be sent to the individual (e.g., national address, email, or university website, etc.).
5. The request form must be submitted directly to the university.

Main Steps for Requesting Access to or Obtaining Public Information:



Firstly: Requests are submitted by filling out the “Public Information Request Form” – electronic or paper – and submitting it to the University.

Secondly: Within a specified period of **thirty (30) days** from the receipt of the request to view or obtain public information, the University shall take one of the following decisions:

1. Approval:

If the request to access or obtain the information is approved fully or partially, the applicant must be notified in writing or electronically of the applicable fees. The University must make this information available to the applicant within a period not exceeding **ten (10) working days** from the date of receiving the payment.

2. Rejection:

If the request to access or obtain the information is refused, the refusal must be in writing or electronic and must include the following information:

- Whether the refusal is total or partial.
- Reasons for the refusal, if possible.
- The right to appeal this decision and instructions on how to utilize this right.

3. Extension:

If the request for access to information cannot be processed within the specified time, the University should extend the period for a reasonable duration depending on the size and nature of the requested information – for example, not exceeding an **additional thirty(30) days** – and provide the applicant with the following information:

- A notice of the extension and the expected completion date.
- Reasons for the delay.
- The right to appeal the extension and instructions on how to do so.

4. Notification:

If the requested information is available on the University's website, or is not within its jurisdiction, the applicant must be notified in writing or electronically with the following information:

- The type of notification – for example, **whether** the requested data is available on the University's website – or is not within its jurisdiction.
- The right to appeal the notice and instructions on how to do so.



Thirdly: If the applicant wishes to appeal the University's refusal of the request, they may submit a written or electronic notice of appeal to the Data Management Office within a period not exceeding **ten (10) working days** from receiving the University's decision. The Appeal Committee at the Data Management Office will review the request, make the appropriate decision, and notify the applicant of the review fees – which will be refunded if the committee approves the request and the appeal decision.

5. General Provisions

Firstly: The Data Management Office at the University is responsible for integrating this policy with the rest of the University's organizational and legislative documents.

Secondly: The University is committed to balancing the right to access information and the necessity of data protection.

Thirdly: The Data Management Office is responsible for monitoring and auditing all University entities' compliance with this policy periodically.

Fourthly: The Data Management Office at the University is responsible for receiving appeals and preparing a mechanism for dealing with them.

Fifthly: All University entities must notify the Data Management Office if a request to view or obtain public data has been refused or the specified time period for providing this information has been extended.

Sixthly: All entities contracting with the University must comply with this policy.

Seventhly: The University has the right to establish additional rules for processing requests related to specific types of public information.

6. Freedom of Information and Open Data

The University of Tabuk, represented by the **Data Governance Unit Office**, has prepared an **Open Data Plan and Policy** as a proactive step in preserving the right to access public information by making available and publishing a specific set of information – as **open data** – before a request to access or obtain it is made.