


<b>Policy Group</b>	Data Governance and Management	<b>Policy Number</b>	UNI-DGM-202	 جامعة زايد ZAYED UNIVERSITY
<b>Classification</b>	Public	<b>Version</b>	1.0	
<b>Responsible Office</b>	VP-CEO	<b>Policy Owner</b>	SFD Director	
<b>Date Approved</b>	3 June 2025	<b>Effective Date</b>	3 June 2025	
<b>Date Last Reviewed</b>	New Policy	<b>Due Date for Next Review</b>	3 June 2028	

## POLICY

### Data Sharing

#### 1. Purpose

This policy outlines the guiding principles for sharing Zayed University data to ensure it is adequately protected according to its sensitivity and risk levels, and in compliance with the University's data regulations and UAE laws.

#### 2. Scope of Application

This policy applies to anyone who has authorized access to Zayed University's information systems, assets, and data. The data users can include Zayed University employees, third-party contractors, service providers, consultants, partners, etc.

#### 3. Definitions

<b>Data Classification Matrix</b>	A document that gives information about the data classification (Restricted, Confidential, Internal, Public) applied to an information asset.
<b>Data Recipient</b>	Any user with whom the data is being shared or the receiver of the data
<b>Data Users</b>	University employees, third-party contractors, service providers, consultants, partners of the University, or anyone authorized to access the University Information Systems and/or University data
<b>DGC</b>	Data Governance Committee
<b>Information Assets</b>	Personal data, sensitive data, research data, and other types of data that are collected, stored, and processed by the University
<b>SFD</b>	Strategy and Future Department
<b>University</b>	Zayed University
<b>VP-CEO</b>	Vice-President and Chief Executive Officer

#### **4. Policy**

**4.1** Zayed University (“**University**”) understands the need for data sharing and is committed to compliance with data protection laws to protect sensitive data, which if lost or compromised can adversely impact the University and its stakeholders.

**4.2** The University will ensure that information assets are properly classified and protected against unauthorized access, disclosure, or loss. Data users at the University will be informed about data-sharing requirements through appropriate communication, training, and contractual terms as necessary.

**4.3** All data users have a responsibility to read, understand, and follow the University’s Data Sharing Policy and Procedures; violations may be subject to disciplinary measures.

**4.3.1** Any claim of ignorance regarding the information contained in this Policy and accompanying Procedures will not be acknowledged as an acceptable excuse for non-compliance.

#### **4.4 Importance of Data Sharing**

The importance of data sharing has been recognized for advancing research, promoting innovation, supporting evidence-based decision-making, and reporting.

##### **4.4.1 Promote Research and Collaboration**

Data sharing can facilitate academic research and collaboration by providing researchers with access to a broader range of data and expertise. This can lead to more innovative and impactful research outcomes.

##### **4.4.2 Improve Quality of Education**

Data sharing can contribute to the improvement of the quality of education by allowing faculty and staff to access and analyze data that can inform decisions and improve teaching and learning outcomes.

#### **4.5 Data Security and Privacy**

All data users are responsible for sharing data by the appropriate security measures as defined in the Data Sharing Procedures to protect against unauthorized access or disclosure of data.

**4.5.1** Violations of the University’s data sharing regulations and/or concerns about unauthorized data sharing activities must be reported to the Data Governance Committee (“**DGC**”).

#### **4.6 Compliance with Data Protection Regulations**

Data users must comply with all relevant UAE Government data protection regulations.

#### **4.7 Terms of Data Sharing**

University users must adhere to the following terms to ensure that data-sharing activities are conducted responsibly and ethically, protecting the privacy and security of individuals and the University.

**4.7.1** Users of University data must:

- a) Respect the privacy and confidentiality of the people whose records are being accessed.

- b) Abide by the data classification matrix and any ethical guidelines that may be imposed on the data.
- c) Comply with applicable laws, regulations, standards, and policies concerning the access, use, disclosure, retention, and disposal of information.
- d) Ensure appropriate permission and authorization to share data have been obtained.
- e) Be transparent about how the data will be used and who will have access to it (data recipients).
- f) Protect sensitive data by using appropriate security measures such as encryption or access controls.
- g) Only share data that is necessary for the intended purpose and avoid sharing unnecessary or extraneous data.
- h) Keep a record of all data-sharing activities, including who accessed the data and for what purpose.

#### **4.7.2 Users of University data must not:**

- a) Reveal information to external parties unless such activity has been approved by the DGC.
- b) Use information for one's own or others' profit or personal gain.
- c) Share data with unauthorized individuals or departments.
- d) Share data for unauthorized purposes or uses.
- e) Share data without first obtaining consent from the relevant individuals (wherever applicable).
- f) Share data without protecting it with appropriate security measures.
- g) Fail to comply with relevant laws and regulations governing data sharing.

#### **4.8 Collaborative Agreements**

When engaging in collaborations with government, external organizations, or other academic institutions, explicit agreements outlining the terms of data sharing are required unless already approved by the DGC.

#### **4.9 Dissemination of Information**

The SFD is responsible for ensuring that the information in this policy is kept up to date, that it is disseminated appropriately, and that it is easily accessible to all employees, third-party contractors, service providers, consultants, partners, etc., as required.

### **5. Related Policies and Laws**

- UNI-DGM-101 Data Governance
- UNI-DGM-201 Data Classification
- UNI-PUB-402 Release of Personal Information and Student Photographs/Videos
- Cabinet Resolution No.73/3 & 1 of 2014 re: Using Social Media by the Employees of Federal Entities
- Federal Law No.2 of 2019 re: The Use of Information and Communication Technology (ICT) in Health Fields
- Federal Law No.15 of 2020 re: Consumer Protection
- Federal Decree-Law No.34 of 2021 re: Combatting Rumors and Cybercrimes
- Federal Decree-Law No.45 of 2021 re: The Protection of Personal Data

- Federal Decree-Law No.46 of 2021 re: Electronic Transactions and Trust Services
- Telecommunications and Digital Government Regulatory Authority (TDRA) policy on Internet Access Management (IAM)
- Government of Dubai Law No.26 of 2015: Regulating Data Dissemination and Exchange in the Emirate of Dubai
- UAE Constitution Article 31

## 6. Administration

SFD is responsible for administering this Policy and the accompanying Procedures in coordination with the DGC. Questions and/or concerns about the University's data-sharing regulations should be forwarded to the DGC.

## 7. Revision History

Date	Revision	Ver.
23 June 2025	Chair of the Board Decision issued (PD#22 of 2025).	
3 June 2025	Approved by FAIAC.	1.0
22 May 2025	Endorsed by UPSC.	
23 October 2024	Endorsed by the Data Governance Committee.	
3 October 2024	New policy drafted.	