جامعة أبوظبي
Abu Dhabi University

PERSONAL DATA PROTECTION AND PRIVACY POLICY

POLICY OVERVIEW

Abu Dhabi University (ADU) is committed to protecting the privacy, confidentiality, integrity, and appropriate use of personal data entrusted to the University. The University is committed to responsible and efficient data management practices, including the promotion of digital-first processes, reduction of unnecessary physical records, and optimization of data handling.

Resolution No	
Executive Order	
Supersedes	
Version Number:	
Date Approved:	
Effective Date:	
Policy Owner:	
Viewing Access Level:	
Next Review Date:	

Change History

Version Number	Change Description	Date	Changed By
01	▪ New Policy		

1. Introduction

This policy establishes the principles, responsibilities, and controls governing the collection, processing, storage, sharing, retention, and disposal of personal data. It aims to ensure that ADU complies with applicable data protection legislation in the United Arab Emirates and follows internationally recognized data protection practices.

The University is committed to responsible and efficient data management practices, including the promotion of digital-first processes, reduction of unnecessary physical records, and optimization of data handling.

Policy Statements

2. Legal and Regulatory Basis

This policy is guided by:

2.1 Federal Decree-Law No. 45 of 2021 Concerning the Protection of Personal Data and its applicable executive regulations and implementing decisions.

2.2 Applicable UAE cybersecurity, electronic transactions, consumer protection, employment, education, and records-management requirements.

2.3 Contractual obligations entered into by ADU.

2.4 Internationally recognized principles of privacy, information security, responsible data governance, and privacy by design.

2.5 Where personal data is processed in another jurisdiction or relates to individuals protected by additional regulations, ADU shall comply with any applicable legal requirements, including contractual and cross-border data-protection obligations.

3. Scope

This policy applies to:

3.1 All ADU campuses, colleges, departments, centers, and administrative units.

3.2 All employees, faculty members, students, contractors, consultants, volunteers, interns, visitors, and third parties processing personal data on behalf of ADU.

3.3 Personal data processed in electronic, paper-based, audio, video, photographic, biometric, or other formats.

3.4 ADU systems, websites, mobile applications, cloud services, learning platforms, research databases, digital communication channels, artificial intelligence tools, and third-party platforms used for university activities.

4. Definitions

4.1 **Personal Data:** Any information relating to an identified or identifiable individual, including names, identification numbers, contact details, academic records, employment records, photographs, recordings, online identifiers, location-related data, and other information that can identify an individual directly or indirectly.

4.2 **Sensitive Personal Data:** Personal data requiring enhanced protection due to its nature or potential impact, including health data, biometric data, financial information, information relating to students, and other categories designated by applicable legislation.

4.3 **Data Subject:** The individual to whom personal data relates.

4.4 Processing**:** Any operation performed on personal data, including collection, recording, organization, storage, retrieval, use, analysis, transfer, sharing, modification, archiving, or deletion.

4.5 **Data Controller:** ADU when it determines the purpose and means of processing personal data.

4.6 **Data Processor:** A third party that processes personal data on behalf of ADU.

4.7 Designated **Responsible Officer:** The officer, committee, or University unit assigned to coordinate implementation of this policy and support privacy-related enquiries and activities.

4.8 **Personal Data Breach:** A security incident resulting in accidental or unlawful loss, destruction, alteration, unauthorized disclosure of, or unauthorized access to personal data.

5. Data Protection Principles

ADU shall process personal data in accordance with the following principles:

5.1 Lawfulness, Fairness, and Transparency

Personal data shall be processed lawfully, fairly, and transparently. Individuals shall be informed of how their personal data is used through clear and accessible privacy notices.

5.2 **Purpose** Limitation

Personal data shall be collected for specific, explicit, and legitimate purposes and shall not be processed for incompatible purposes unless permitted by law or supported by an appropriate legal basis.

5.3 Data Minimization
Only the personal data necessary to achieve the intended purpose shall be collected and processed.

5.4 **Accuracy**
Reasonable steps shall be taken to ensure that personal data is accurate, complete, and updated where necessary.

5.5 **Storage** Limitation
Personal data shall be retained only for as long as necessary to fulfil its intended purpose, comply with legal requirements, or protect the University's legitimate interests.

5.6 **Security** and Confidentiality
Appropriate technical, organizational, and physical safeguards shall be applied to protect personal data against unauthorized access, misuse, alteration, loss, or disclosure.

5.7 **Accountability**
ADU shall maintain appropriate records, assign clear responsibilities, conduct periodic reviews, and be able to demonstrate compliance.

5.8 **Privacy** by Design and by Default
Privacy considerations shall be incorporated into the planning, procurement, design, implementation, and operation of systems, services, research projects, artificial intelligence applications, and digital initiatives.

6. Governance and Responsibilities

6.1 Approving Authority
The approving authority shall endorse this policy and ensure that data protection is embedded within the University's governance framework.

6.2 Governance and Coordination
ADU shall designate appropriate University units to coordinate implementation of this policy and support privacy-related enquiries, complaints, and awareness activities.
The designated University units responsible for governance and coordination shall:

- 6.2.1 Monitor compliance with this policy and applicable legislation.
- 6.2.2 Advise University units on data protection requirements.
- 6.2.3 Receive and coordinate responses to data-subject requests and complaints.
- 6.2.4 Maintain oversight of the University's personal-data inventory.
- 6.2.5 Advise on Data Protection Impact Assessments.
- 6.2.6 Review personal-data breaches and coordinate regulatory and individual notifications where required.
- 6.2.7 Support training and awareness activities.
- 6.2.8 Provide periodic reports to the approving authority or designated governance committee.

6.3 Digital Advancement Transformation and AI (DATA)

DATA shall implement and maintain appropriate cybersecurity controls, access management procedures, secure backups, monitoring arrangements, incident-response processes, and technical safeguards.

6.4 University Units

Each college, department, and administrative unit shall:

- 6.4.1 Identify the personal data it collects and processes.
- 6.4.2 Ensure that processing has an appropriate legal basis.
- 6.4.3 Follow approved retention and disposal requirements.
- 6.4.4 Limit access to authorized individuals.
- 6.4.5 Report suspected breaches immediately.
- 6.4.6 Cooperate with relevant University authorities in audits, assessments, and data-subject requests.

6.5 Employees, Faculty Members, and Contractors

All individuals handling personal data shall:

- 6.5.1 Process data only for authorized University purposes.
- 6.5.2 Protect passwords, devices, documents, and confidential information.
- 6.5.3 Avoid sharing personal data through unauthorized channels.
- 6.5.4 Complete required training.
- 6.5.5 Report suspected data breaches or misuse without delay.

7. Inventory of Personal Data Processing Activities

ADU shall develop and progressively maintain a processing register, beginning with priority systems. The register shall include, as appropriate:

- 7.1 The responsible University unit.
- 7.2 Categories of data subjects.
- 7.3 Types of personal data collected.
- 7.4 Purpose of processing.
- 7.5 Legal basis for processing.
- 7.6 Authorized users and recipients.
- 7.7 Data processors and third-party service providers.
- 7.8 Data retention periods.
- 7.9 Cross-border transfers.
- 7.10 Security safeguards.
- 7.11 Disposal methods.
- 7.12 Whether sensitive personal data is processed.
- 7.13 Whether automated decision-making or artificial intelligence is used.
- 7.14 Whether a Data Protection Impact Assessment is required.
- 7.15 The register shall be reviewed and updated periodically.

8. Lawful Processing and Consent

ADU shall process personal data only where there is an appropriate legal basis, such as:

- 8.1 The individual's valid consent.
- 8.2 Performance of a contract or delivery of an educational or administrative service.
- 8.3 Compliance with a legal or regulatory obligation.
- 8.4 Protection of the vital interests of an individual.
- 8.5 Performance of an authorized institutional function.
- 8.6 A legitimate University interest that does not override the individual's rights and freedoms.

8.7 Another basis permitted by applicable legislation.
8.8 Where processing is based on consent:
8.9 Consent shall be clear, specific, informed, and recorded.
8.10 Consent requests shall be written in plain and accessible language.
8.11 Individuals shall be able to withdraw consent through a reasonable and straightforward process.
8.12 Withdrawal of consent shall not affect the lawfulness of processing performed before the withdrawal.
8.13 Separate consent shall be obtained where required for materially different purposes.
8.14 Additional safeguards shall apply when processing sensitive personal data.

9. Privacy Notices

ADU shall provide privacy notices at appropriate points of data collection, including through application forms, employment documentation, University websites, mobile applications, research activities, events, digital platforms, and online services.

Privacy notices shall explain, as applicable:
9.1 The categories of personal data collected.
9.2 The purposes of processing.
9.3 The legal basis for processing.
9.4 The recipients or categories of recipients.
9.5 Relevant third-party processors.
9.6 Retention periods or retention criteria.
9.7 Cross-border transfers and applicable safeguards.
9.8 The individual's rights.
9.9 The use of automated processing or profiling.
9.10 How to contact ADU and the University's designated reporting channel. How to submit a complaint.

10. Rights of Individuals

Subject to applicable legislation and reasonable identity-verification procedures, individuals may request:

Information about how their personal data is processed.
10.1 Access to their personal data.
10.2 Correction or completion of inaccurate personal data.
10.3 Erasure of personal data where legally permitted.
10.4 Restriction or cessation of processing in applicable circumstances.
10.5 Withdrawal of consent where processing is based on consent.
10.6 Transfer of eligible personal data in a structured and machine-readable format where applicable.
10.7 Objection to direct marketing.
10.8 Review of significant decisions made through automated processing, including the involvement of an appropriate human reviewer where required.
10.9 ADU shall maintain a documented procedure for receiving, verifying, tracking, responding to, and closing requests within applicable legal timeframes.

11.11. Information Security Measures

ADU shall implement risk-based security measures appropriate to the sensitivity and volume of personal data processed. These shall include, where appropriate:

11.1 Role-based access controls and least-privilege access.
11.2 Multi-factor authentication for relevant systems.
11.3 Encryption or equivalent safeguards for sensitive data at rest and in transit.
11.4 Secure password and identity-management controls.
11.5 System logging, monitoring, and periodic access reviews.
11.6 Secure backup, recovery, and business-continuity arrangements.
11.7 Endpoint security and vulnerability management.
11.8 Secure configuration of systems and cloud services.
11.9 Data classification and handling requirements.
11.10 Pseudonymization or anonymization where appropriate.
11.11 Secure disposal of electronic and paper records.
11.12 Periodic testing, auditing, and evaluation of security controls.

12. Personal Data Breach Management

12.1 All suspected or confirmed personal-data breaches shall be reported immediately through helpdesk@adu.ac.ae.
12.2 ADU shall maintain a breach management procedure.
12.3 All breaches and suspected breaches shall be recorded, including those that do not require external notification.

13. Third-Party Processors and Service Providers

Before appointing a third party to process personal data, ADU shall conduct an appropriate due-diligence review.

Contracts with data processors shall address:

13.1 The nature, purpose, and duration of processing.
13.2 Categories of personal data and data subjects.
13.3 Confidentiality obligations.
13.4 Security requirements.
13.5 Restrictions on subcontracting.
13.6 Breach-reporting obligations.
13.7 Liability of the Third-party processors and monetary compensation in case of breach of confidentiality obligations.
13.8 Interim measures that can be taken against the Third-party processors in case of breach of confidentiality obligations.
13.9 Data-subject request support.
13.10 Audit and compliance rights.
13.11 Retention, return, and secure deletion of data.
13.12 Cross-border data-transfer requirements.
13.13 Responsibilities upon termination of the agreement.
13.14 Third parties shall process ADU personal data only in accordance with documented instructions and applicable legislation.

14. Cross-Border Data Transfers

Personal data shall be transferred outside the UAE only where there is an appropriate legal basis and adequate safeguards.

Before transferring personal data internationally, ADU shall assess:

14.1 The necessity and justification for the transfer, including the specific purpose, scope, and legal basis for transferring the personal data outside the UAE, and whether the same purpose can reasonably be achieved while keeping the personal data secured and protected within the UAE.
14.2 The destination country.
14.3 The recipient organization.
14.4 The sensitivity and volume of the data.
14.5 Applicable contractual protection.
14.6 Security measures.
14.7 The availability and adequacy of contractual protections, including confidentiality obligations, liability provisions, and appropriate remedies in the event of unauthorized disclosure, misuse, or breach of personal data.
14.8 The interim protective measures available to ADU in the event of a suspected or confirmed breach, including suspension of processing, restriction of access, containment actions, investigation support, notification obligations, and corrective measures.
14.9 The specific purpose, scope, and duration of the transfer, including whether the transfer is limited to what is necessary for the approved purpose.
14.10 The legal, regulatory, operational, and institutional risks associated with the transfer, including risks arising from the destination country, recipient organization, applicable laws, and the nature of the personal data.
14.11 The retention, return, deletion, or secure disposal obligations applicable to the transferred personal data during the relationship and upon termination or expiry of the relevant agreement.

For cross-border transfers involving sensitive personal data, high-risk processing, or significant volumes of personal data, the relevant University authorities shall review the transfer assessment and confirm that appropriate safeguards, approvals, and documented justifications are in place before the transfer proceeds.

15. Data Retention and Secure Disposal

15.1 ADU shall maintain a Personal Data Retention Schedule based on legal, regulatory, academic, research, operational, and contractual requirements.
15.2 When personal data is no longer required, it shall be securely deleted, destroyed, anonymized, or archived in accordance with approved procedures.
15.3 University units shall not retain personal data indefinitely without a documented justification.

16. Research Activities

Personal data used for research shall be processed ethically, lawfully, and securely.

Researchers shall:

16.1 Obtain required institutional approvals.

16.2 Follow applicable research-ethics procedures.
16.3 Use anonymized or pseudonymized data where feasible.
16.4 Limit access to authorized research-team members.
16.5 Obtain informed consent where required.
16.6 Establish secure data-storage and disposal arrangements.
16.7 Address cross-border transfers and collaboration agreements.
16.8 Complete a Data Protection Impact Assessment for high-risk activities where required.

17. Artificial Intelligence and Automated Decision-Making

ADU shall apply enhanced safeguards when artificial intelligence, analytics, profiling, or automated decision-making tools process personal data. AI output affecting individuals shall be subject to appropriate human oversight where required.

Before implementation, the unit responsible shall assess:

17.1 The purpose and necessity of the proposed processing.
17.2 The categories and sensitivity of personal data.
17.3 Risks of unauthorized disclosure, inaccurate results, bias, or unfair outcomes.
17.4 Whether individuals should be notified.
17.5 Whether consent or another legal basis is required.
17.6 Whether human oversight is required.
17.7 Whether a Data Protection Impact Assessment is required.
17.8 Security, vendor, cloud-hosting, and cross-border transfer risks.
17.9 Personal data shall not be uploaded to unauthorized generative artificial intelligence tools or external platforms.

18. Data Protection Impact Assessments

A Data Protection Impact Assessment shall be completed before introducing processing activities that may create a high risk for individuals, particularly where activities involve:

18.1 Large volumes of personal or sensitive data.
18.2 Biometric technologies.
18.3 Artificial intelligence or automated decision-making.
18.4 Profiling or systematic monitoring.
18.5 New digital platforms.
18.6 Cloud services involve significant personal data.
18.7 Research involving sensitive personal data.
18.8 Cross-border transfers with elevated risks.
18.9 The assessment shall document the purpose, necessity, risks, safeguards, responsible parties, and approval requirements. Relevant University authorities shall be consulted where appropriate.

19. Photography, Video Recording, and Digital Communications

ADU shall apply appropriate privacy safeguards when capturing, using, or publishing photographs, videos, recordings, testimonials, or personal information through websites, social-media platforms, events, and marketing materials. Consent or another appropriate legal basis shall be obtained where required.

20. Training and Awareness

20.1 ADU shall provide periodic data protection awareness activities appropriate to staff roles.

21. Complaints and Reporting Concerns

Individuals may submit concerns, complaints, or suspected violations through: Privacy-related concerns or complaints may be submitted through the University's designated reporting channel. ADU shall review concerns promptly, maintain confidentiality, document actions taken, and protect individuals who report concerns in good faith.

22. Implementation and internal exception

Any exception to this policy shall be documented, risk-assessed, approved by the relevant University authority, and limited to a defined period. Exceptions shall include the justification, scope, compensating controls, accountable owner, expiry date, and review requirements. Approved exceptions shall be reviewed periodically and withdrawn where the justification no longer applies or the risk is no longer acceptable.

23. Supporting Unites:

Digital Advancement Transformation and AI (DATA), Human Resources, Registrar's Office, Student Affairs, Research Office, Marketing and Communications, and all colleges and administrative units

24. Related and supporting policies and documents which form an integral part of this Policy

- ADU Sustainable Investment Policy.
- ADU Sustainability Strategic Plan.
- ADU Code of Conduct and Ethics.
- ADU Procurement and Purchasing Policy.
- ADU AI AND ADVANCED DIGITAL TECHNOLOGIES GOVERNANCE POLICY.

Exceptions

For any conditions/circumstances and/or exceptions outside the conditions stated in this policy, a request shall be presented to the Board of Directors for decision.

Authorization

This policy was authorized by the **University Chancellor.**