To: All Colleges
Departments, Divisions, and Units
Subject: Data Protection Policy

1. Introduction and Purpose

University of AlKafeel places the utmost importance on protecting the personal data of students, staff, and faculty members to ensure privacy and digital security for all stakeholders. This policy aims to activate the Data Protection Framework 2026 as a fundamental pillar for the secure and responsible management of digital information.

The purpose of this policy is to address risks associated with data processing, ensure compliance with national data protection laws, align with international best practices, and safeguard the rights of all data subjects.

2. Core Principles

This policy is based on the following key principles to achieve secure and responsible data management:

- Legality and Transparency: Processing personal data in a lawful and transparent manner, while informing data subjects of the purposes of processing.
- Data Minimization: Collecting and processing only the minimum necessary data to achieve the specified purposes.
- Accuracy: Maintaining accurate data and updating it when required.
- Security: Protecting data against unauthorized access, damage, or loss through appropriate technical and organizational measures.
- Data Subject Rights: Enabling students and staff to access, correct, or withdraw consent regarding their personal data.

3. Investment Strategies

The university invests its resources in implementing best practices for data protection through:

- Developing Digital Infrastructure: Adopting secure systems for university-wide data management.
- Applying Technical Controls: Using encryption, backups, and access control systems to ensure data security.
- Awareness and Training: Organizing training programs and workshops to enhance the data protection culture among all staff and students.

4. Exclusion List (Negative Screening)

The university is committed to avoiding practices that expose personal data to risks, including:

- Sharing personal data without proper consent or legitimate purpose.
- Storing data on insecure media or outside official university systems.

- Ignoring data subject rights regarding access, correction, or objection.

5. Priority Investment Sectors

The university focuses its data protection efforts on the following areas:

- Academic and Administrative Data: Securing student, staff, and faculty records.
- Research Information: Ensuring the security of research files and scientific data.
- Digital Portal Systems: Protecting student, faculty, and administrative portals from unauthorized access or data leaks.

6. Governance and Reporting

The university manages data protection through:

- Appointing a Data Protection Officer (DPO) to monitor compliance and manage risks.
- Continuous monitoring of digital systems and periodic auditing of data protection procedures.
- Preparing regular reports on compliance levels and data protection policies across all academic and administrative units.

7. Divestment Policy

The university commits to withdrawing any activities, systems, or applications found to contribute to:

- Violations of personal data privacy or manipulation of data.
- Weak cybersecurity that may threaten the integrity of institutional data.

8. Review Clause

This policy is subject to periodic review every five years. The 2026 version represents an official revision since its initial adoption, ensuring continued alignment with international best practices, national laws, regulatory trends, and the strategic vision of University of AlKafeel.

N. ALDAHA

Prof.Dr. Nawras M. Shaheed Aldahan
Chancellor of the University
12/01/2026

إلى/ الكليات كافة

الاقسام والشعب والوحدات كافة

م/ سياسة حماية البيانات

1. المقدمة والغرض

تولي جامعة الكفيل أهمية قصوى لحماية البيانات الشخصية للطلاب والموظفين وأعضاء هيئة التدريس، لضمان الخصوصية والأمن الرقمي لجميع الأطراف. تهدف هذه السياسة إلى تفعيل إطار حماية البيانات كركيزة أساسية لإدارة المعلومات الرقمية بشكل آمن ومسؤول. الغرض من هذه السياسة هو معالجة المخاطر المرتبطة بمعالجة البيانات، وضمان التوافق مع القوانين الوطنية لحماية البيانات وأفضل الممارسات الدولية، وحماية حقوق جميع أصحاب البيانات.

2. المبادئ الأساسية

تستند السياسة إلى المبادئ الجوهرية التالية لتحقيق إدارة بيانات آمنة ومسؤولة:

- الشرعية والشفافية :معالجة البيانات بطريقة قانونية وشفافة، مع إعلام أصحاب البيانات بأغراض الاستخدام .
- تقليل البيانات :جمع ومعالجة الحد الأدنى فقط من البيانات الضرورية لتحقيق الأغراض المحددة .
- الدقة :الحفاظ على دقة البيانات وتحديثها عند الحاجة .
- الأمن :حماية البيانات من الوصول غير المصرح به، التلف، أو الفقدان من خلال التدابير التقنية والتنظيمية المناسبة .
- حقوق أصحاب البيانات :تمكين الطلاب والموظفين من الوصول إلى بياناتهم وتصحيحها أو سحب الموافقة عند الحاجة .

3. استراتيجيات الاستثمار

تستثمر الجامعة مواردها في تطبيق أفضل الممارسات لحماية البيانات من خلال:

- تطوير البنية التحتية الرقمية :اعتماد أنظمة آمنة لإدارة البيانات على مستوى الجامعة .
- تطبيق الضوابط التقنية :استخدام التشفير، النسخ الاحتياطي، وأنظمة الوصول المحدد لضمان حماية البيانات .
- التوعية والتدريب :تنظيم برامج تدريبية وورش عمل لتعزيز ثقافة حماية البيانات لدى جميع الموظفين والطلاب .

4 .قائمة الاستبعادات (الفحص السلبي)

تلتزم الجامعة بالابتعاد عن الممارسات التي تعرض البيانات الشخصية للمخاطر، بما في ذلك:

- مشاركة البيانات الشخصية بدون إذن أو غرض مشروع .
- تخزين البيانات على وسائل غير آمنة أو خارج نطاق الأنظمة الرسمية للجامعة .
- تجاهل حقوق أصحاب البيانات في الوصول أو التصحيح أو الاعتراض.

5 .القطاعات ذات الأولوية للاستثمار

تركز الجامعة جهودها لحماية البيانات في المجالات التالية:

- البيانات الأكاديمية والإدارية :حماية سجلات الطلاب، الموظفين، والكوادر التدريسية .
- المعلومات البحثية :ضمان أمان ملفات البحوث والبيانات العلمية .
- أنظمة البوابات الرقمية :تأمين بوابات الطلبة، التدريسيين، والإداريين ضد أي اختراق أو تسريب بيانات .

6 .الحوكمة وإعداد التقارير

تتولى الجامعة إدارة حماية البيانات من خلال:

- تعيين مسؤول حماية البيانات (DPO) لمتابعة الامتثال وإدارة المخاطر .
- المراقبة المستمرة للأنظمة الرقمية والتدقيق الدوري على إجراءات حماية البيانات .
- إعداد تقارير دورية حول مستوى الامتثال وسياسات حماية البيانات لجميع الوحدات الأكاديمية والإدارية .

7 .سياسة التخارج (سحب الاستثمارات)

تلتزم الجامعة بسحب أي أنشطة أو أنظمة أو تطبيقات يتم اكتشاف مساهمتها في:

- انتهاك خصوصية البيانات الشخصية أو التلاعب بها .
- ضعف الأمان السيبراني الذي قد يهدد سلامة البيانات المؤسسية .

8. بند المراجعة

تخضع هذه السياسة للمراجعة الدورية كل خمس سنوات. وتمثل نسخة عام 2026 مراجعة رسمية للسياسة منذ اعتمادها الأولي، على أن تضمن المراجعات اللاحقة استمرار توافقها مع أفضل الممارسات العالمية، القوانين الوطنية، والتوجهات التنظيمية، والرؤية الاستراتيجية لجامعة الكفيل.

أ.د نورس محمد شهيد الدهان
رئيس الجامعة
2026/01/12