



جامعة المستقبل
Mustaqbal University
أول جامعة أهلية بمنطقة القصيم

سياسة حفظ المعلومات وتداولها

إعداد

إدارة الإعلام والاتصال المؤسسي

إدارة تقنية المعلومات

وحدة الإحصاء والمعلومات

الإصدار الأول

يناير 2025



بطاقة تعريف السياسة

سياسة حفظ المعلومات وتداولها	مسمى السياسة
UOM-MED-MICD-POL-001-V1-Ar	الكوود
إدارة الإعلام والاتصال المؤسسي	المالك
1. نظام حماية البيانات الشخصية الصادر بالمرسوم الملكي رقم م/ 19 وتاريخ 2/9/1443 هـ والمعدل بموجب المرسوم الملكي رقم م/ 148 وتاريخ 9/5/1444 هـ 2. اللائحة التنفيذية لنظام حماية البيانات الشخصية الصادرة بقرار رقم 1516 وتاريخ 19/2/1445 هـ. 3. وثيقة سياسة مشاركة البيانات الصادر من الهيئة السعودية للبيانات والذكاء الاصطناعي والمحدثة بالإصدار 2.	المرجعية
إرشاد منسوبي الجامعة والطلبة بشأن سياسة حفظ المعلومات والتعامل معها وإجراءات تداولها	الغرض
جميع وحدات الجامعة الأكاديمية والإدارية	نطاق التنفيذ
المدير التنفيذي للجامعة	الاعتماد
يناير 2025 م	الإصدار الأول
مخطط مراجعة كل سنتين	المراجعة
يناير 2025 م	الإصدار الحالي

المحتويات

مقدمة

1. جهات حفظ المعلومات وتداولها بالجامعة
- 1.1 أنواع المعلومات وسياسة النشر
- 2.1 جهات حفظ المعلومات

-
- 3.1 جهات تبادل المعلومات داخليا وخارجيا
 2. السياسات المتعلقة بالبوابة الإلكترونية
 - 1.2 مفاهيم البوابة الإلكترونية
 - 2.2 شروط الاستخدام
 - 3.2 حجز النطاقات الفرعية
 - 4.2 صلاحية إدخال المحتوى وتحديثه
 - 5.2 النشر على البوابة
 - 6.2 الإشراف والتدريب
 - 7.2 السياسات المتعلقة بالشبكة الداخلية
 3. سياسة خصوصية واستخدام البيانات بجامعة المستقبل
 - 1.3 الموافقة على سياسة الخصوصية
 - 2.3 التغييرات على سياسة الخصوصية
 - 3.3 البيانات الشخصية التي يتم جمعها
 - 4.3 طرق جمع البيانات الشخصية
 - 5.3 أسباب جمع البيانات
 - 6.3 كيفية استخدام البيانات
 - 7.3 مشاركة البيانات الشخصية
 - 8.3 المسوغات النظامية
 - 9.3 تخزين البيانات وإتلافها
 - 10.3 حقوق أصحاب البيانات
 - 11.3 بيانات التواصل
- الخاتمة**



مقدمة

تسعى جامعة المستقبل إلى تعزيز بيئة معلوماتية آمنة وموثوقة تدعم أعمالها الأكاديمية والإدارية والبحثية، وتضمن سلامة تداول المعلومات داخل الجامعة وخارجها. وانطلاقاً من دور الجامعة في حماية بياناتها وممتلكاتها المعلوماتية، يأتي هذا الدليل ليضع الإطار التنظيمي والسياسات والإجراءات التي تحكم حفظ المعلومات وتداولها، بما يضمن توحيد الممارسات ورفع مستوى الحوكمة والامتثال.

ويهدف هذا الدليل إلى تحديد الجهات المخولة بحفظ المعلومات وتداولها، وتصنيف أنواع المعلومات وفق درجة سريتها، وتوضيح السياسات المتعلقة بالبوابة الإلكترونية والشبكة الداخلية، إضافة إلى تنظيم عمليات النشر، وإدارة المحتوى، وضوابط استخدام الأنظمة التقنية. كما يوضح الدليل مسؤوليات الجهات المختلفة داخل الجامعة في التعامل مع المعلومات، بما يتوافق مع الأنظمة الوطنية ذات العلاقة، مثل نظام حماية البيانات الشخصية، وسياسات الأمن السيبراني، وضوابط مشاركة البيانات.

وتلتزم الجامعة من خلال هذا الدليل بتطبيق أفضل الممارسات في إدارة المعلومات، وضمان حماية خصوصية الأفراد، والمحافظة على سرية البيانات، وتعزيز الشفافية والمسؤولية في تداول المعلومات، بما يساهم في دعم مسيرة الجامعة وتحقيق أهدافها الاستراتيجية.

1. جهات حفظ المعلومات وتداولها بالجامعة

1.1 أنواع المعلومات وسياسة النشر

تنقسم معلومات الجامعة إلى فئات رئيسة من حيث درجة العمومية والسرية، ويمكن عرضها بشكل مبسط كالتالي:

معلومات عامة: هي المعلومات التي تتيحها الجامعة للجمهور دون قيود، وغالباً تُنشر في الموقع الرسمي أو الأدلة التعريفية. أمثلة على ذلك:

- الرؤية والرسالة والقيم والأهداف الإستراتيجية للجامعة .
- الأنظمة واللوائح والسياسات المنشورة، مثل سياسات البيانات المفتوحة أو أدلة المجالس والهيكل التنظيمي.

- برامج الدراسة، وشروط القبول العامة، والتقويم الأكاديمي، وأخبار الجامعة وفعاليتها.

معلومات داخلية غير سرية: هي معلومات ليست للنشر العام لكنها متاحة لمنسوبي الجامعة (أعضاء هيئة تدريس، موظفين، أحياناً طلاب) عبر البوابات الداخلية. أمثلة على ذلك:

- محاضر بعض المجالس الأكاديمية والإدارية التي لا تُنشر للعموم .
- تقارير الأداء الداخلية، وخطط الأقسام التفصيلية، وإجراءات العمل التشغيلية .
- بعض قواعد البيانات الإدارية والتنظيمية التي لا تمس خصوصية الأشخاص مباشرة.

معلومات سرية: هي المعلومات التي يترتب على إفشائها ضرر على الأفراد أو الجامعة، وتحميها لوائح حماية البيانات والأنظمة الإلكترونية. أمثلة على ذلك:

- البيانات الشخصية للطلبة وأعضاء هيئة التدريس والموظفين (السجلات الأكاديمية، أرقام الهوية، البيانات المالية، السجلات الصحية) .
- بيانات الدخول إلى الأنظمة، وأي بيانات تمس أمن المعلومات أو الأمن السيبراني أو الأمن الداخلي/المالي للجامعة.

معلومات شديدة السرية: هذه فئة فرعية أعلى حساسية داخل “السرية”، وغالباً تُقيد بصلاحيات محدودة جداً.



أمثلة على ذلك:

- خطط الطوارئ والأمن والسلامة التي قد يمس إفشاؤها الأمن .
- بعض العقود المالية الكبرى، والتحقيقات الداخلية، وتقارير المراجعة أو القضايا القانونية قبل حسمها .
- أي معلومات تحددها الجامعة في سياساتها بأنها “مقيدة” أو “سرية للغاية”.

ملاحظات تنظيمية مهمة

- تربط الجامعة بين هذه الفئات وسياسات حماية الخصوصية، الأمن السيبراني، والبيانات المفتوحة، بحيث تحدد ما يجوز نشره وما يجب حمايته وطرق التعامل معه.
- يمكن الرجوع إلى سياسة أمن المعلومات في دليل "إدارة تقنية المعلومات" بالجامعة وسياسة الخصوصية على البوابة، لمعرفة كيفية حماية المعلومات الشخصية والسرية.

2.1 جهات حفظ المعلومات

توجد الكثير من الجهات في الجامعة المخولة بحفظ المعلومات ورقيا وإلكترونيا ومن أهمها:

- مكتب مدير الجامعة
- مكاتب السكرتارية
- إدارة الوثائق والسجلات
- نظم الحفظ الإلكتروني
- إدارة الجودة والاعتماد
- وحدة الإحصاء والمعلومات

3.1 جهات تبادل المعلومات داخليا وخارجيا

الكثير من الجهات مخولة بتبادل المعلومات داخليا ومنها:

- مكتب مدير الجامعة
- مكاتب السكرتارية
- منصة الجامعة الإلكترونية
- إدارة الجودة والاعتماد
- وحدة الإحصاء والمعلومات
- إدارة الإعلام والاتصال المؤسسي

بينما تحدد الجامعة جهات معينة وأشخاص لهم صلاحيات تبادل المعلومات خارجياً، بعد التأكد من جواز نشرها، وعلى رأسها:

- مكتب رئيس الجامعة
- إدارة الإعلام والاتصال
- ضباط اتصال يفوضون في ذلك من الإدارة العليا.



2. السياسات المتعلقة بالبوابة الإلكترونية

1.2 مفاهيم البوابة الإلكترونية

- البوابة هي الموقع الإلكتروني لجامعة المستقبل وكل ما يتبع له من مواقع نشر المحتوى سواء أكان موقع كلية أم إدارة أم موقعاً خاصاً بعضو هيئة تدريسي أو موظف أو طالب.
- شروط الاستخدام هي جميع الشروط والضوابط التي يجب أن تراعى عند استخدام البوابة الإلكترونية بجامعة المستقبل.
- المحتوى هو النصوص أو الرسوم البيانية أو الإعلانات أو الروابط أو غيرها من المواد كأخبار الجامعة، وفعاليات الجامعة، والمرئيات، وبيانات التواصل بمنسوبي الجامعة، والمقررات الدراسية والمقالات المنشورة.
- الروابط الخارجية هي الروابط التي تنقل التصفح إلى صفحات لا تتبع لبوابة جامعة المستقبل.

2.2 شروط الاستخدام

- تعد البوابة الموقع الرسمي الوحيد لجامعة المستقبل وتدار من قبل إدارة تقنية المعلومات ممثلة بقسم البرمجيات وإدارة البوابة الإلكترونية، ويدار المحتوى فيها من خلال الكليات، والإدارات ومراكز الجامعة وكلاهما يعبر عن نفسه.
- تتيح الجامعة شروط الاستخدام للبوابة الإلكترونية على جميع صفحات البوابة.
- يجب على المستخدم معرفة أن استخدامه لبوابة جامعة المستقبل يعد قبولاً منه بشروط استخدام البوابة، فإذا كان لا يقبلها بالكامل فإن دخوله لهذا الموقع أو أي موقع فرعي يعد تعدياً وعليه أن يتوقف عن استخدامه فوراً.

3.2 حجز النطاقات الفرعية

- استضافة مواقع جامعة المستقبل على الشبكة العالمية يتم من خلال الجامعة، أو من خلال جهات حكومية أخرى، أو من خلال مقدمي خدمات الاستضافة الذين رخصت لهم هيئة الاتصالات وتقنية المعلومات. على أن تكون الاستضافة داخل المملكة، وأن يتضمن العقد المبرم بين الطرفين ضوابط لضمان سرية المعلومات.

- يحق لكل جهة بالجامعة حجز نطاق أو اسم مختصر ليكون تابع لمجال الجامعة (uom.edu.sa) وذلك بتقديم خطاب رسمي إلى (إدارة تقنية المعلومات) موضح فيه الاسم المختصر المطلوب حجزه.
- لا يحق لأي جهة بجامعة المستقبل إنشاء موقع إلكتروني تابع لها خارج المجال (uom.edu.sa).

4.2 صلاحية إدخال المحتوى وتحديثه

- تقع مسؤولية الاضافة أو الحذف أو التعديل على علامات التبويب بالصفحة الرئيسية لبوابة الجامعة على عاتق قسم البرمجيات والبوابة الالكترونية التابعة لإدارة تقنية المعلومات بجامعة المستقبل أو من تنيها.
- تقع مسؤولية إدارة صحيفة الجامعة الإلكترونية على إدارة الاعلام والاتصال المؤسسي بالجامعة حيث إن لديه كامل الصلاحية في نشر وتحديث محتويات الصحيفة الإلكترونية وكذلك كل ما هو متعلق بالأخبار والفعاليات والندوات والمؤتمرات والمقالات وما يندرج تحتها من خدمات خاصة بها.
- على اي جهة من جهات جامعة المستقبل ترغب بنشر اخبار أو فعاليات أو ندوات أو مقالات أو مؤتمرات على الصفحة الرئيسية لبوابة الجامعة التواصل مع مركز الاعلام والاتصال بالجامعة بشكل رسمي.
- في حال وجود إضافة برمجية (كإضافة نموذج تسجيل حضور على سبيل المثال لا الحصر)، يجب أن يتم تزويد قسم البرمجيات والبوابة الالكترونية بإدارة تقنية المعلومات بخطاب رسمي عبر وسائل الاتصالات الإدارية يحتوي على الطلبات بمدة لا تقل عن ثلاث أسابيع قبل تاريخ انعقاد المؤتمر أو الفعالية، وبغير ذلك لن يتم النظر الي الطلب.
- كل جهة من جهات الجامعة لديها موقع مستقل بصلاحيه إدارته بشكل كامل، بحيث تقع مسؤولية نشر وتحديث المحتوى الإلكتروني الخاص بكل جهة على عميد أو مدير الجهة المسؤول ويتحمل مسؤولية نشر وتحديث كامل محتوياته، كما أن لكل عضو هيئة تدريس أو موظف أو طالب أو طالبة موقع مستقل.



- لا تلتزم إدارة تقنية المعلومات بمراجعة الروابط الخارجية المتصلة بالبوابة، ولا تتحمل الإدارة مسؤولية المحتوى أو الخدمات التي تقدمها المواقع المسجلة خارج نطاق البوابة الرسمية للجامعة.

5.2 النشر على البوابة

- تعد البوابة وسيلة نشر إلكتروني لجميع منسوبي الجامعة وقطاعاتها وعليهم استخدامها فيما يعود بالنفع على الجامعة ومنسوبيها وقطاعاتها المختلفة وبما لا يخل بأي شكل من الأشكال بسمعة الجامعة ومنسوبيها أو يعرضهم للمساءلة القانونية.
- كل المحتوى المنشور في صفحات البوابة يجب أن يتوافق مع حقوق النشر، وعليه يمنع نشر الآتي دون الحصر:
 - أي مواد إلكترونية غير مملوكة لصاحب الصفحة ولها حقوق نشر.
 - البحوث المنشورة في مؤتمرات علمية ومجلات علمية.
 - الكتب والمؤلفات المتوفرة بأي صيغ إلكترونية.
 - المحتوى غير الملائم ويشمل الآتي دون الحصر:
 - ما يحتوي على لهجة نابية أو متهجمة أو عنصرية أو مهددة سواء أكان نصاً أم صورة أو فكرة.
 - ما يخالف أنظمة الدولة والجامعة أو أعراف المجتمع.
 - ما يتعرض لخصوصية الآخرين بأي شكل من الأشكال.
- على كل جهة بالجامعة لها موقع تابع لبوابة الجامعة التأكد من تحديث محتوى الصفحات والمواد بما في ذلك الأخبار ومعلومات الاتصال وأرقام الهواتف والبريد الإلكتروني ووصف المواد وغيرها من المعلومات.
- على الجميع استخدام قواعد اللغة المستخدمة لإنشاء الصفحة أو المادة الإلكترونية والتأكد من سلامتها وخلوها من الأخطاء.
- تحتفظ إدارة تقنية المعلومات بالحق في التغيير أو الحذف للمعلومات الواردة في أي موقع تحت مظلة الجامعة في أي وقت دون سابق إنذار في حال الإخلال بسياسات البوابة للنشر وإدارة المحتوى.

6.2 خصوصية معلومات الطلاب على البوابة:

- على إدارة تقنية المعلومات بجامعة المستقبل إتاحة سياسة الخصوصية على جميع صفحات البوابة، توضيحاً لحقوق وواجبات موقع الجامعة والمواقع التابعة لها ومستخدميها، وعليه تلتزم جامعة المستقبل بحماية سرية وخصوصية المستخدم.
- تحتوي سياسات الخصوصية على كيفية تعامل جامعة المستقبل مع معلومات المستخدم الشخصية فيما يتعلق بالبيانات سواء أكانت على الإنترنت أم على أجهزة الكمبيوتر فقط.
- تتصل بعض الروابط على موقع جامعة المستقبل بمواقع أخرى غير تابعة للجامعة (ليست ضمن المجال (uom.edu.sa) وهذه المواقع لا تعمل وفقاً لسياسة الخصوصية المتبعة في موقع جامعة المستقبل لذا على الزائر مراجعة سياسة الخصوصية الخاصة بتلك المواقع قبل الكشف عن أي معلومات شخصية تدل على صاحبها.

7.2 الإشراف والتدريب

- يحق لكل جهة بالجامعة أن تخصص مشرفاً أو أكثر خاصاً بها، حيث يعطى هذا المشرف الصلاحيات اللازمة على حسابه الجامعي المستخدم في نظام الدخول ويكون بذلك المسئول عن الموقع الإلكتروني للجهة ومحتواه وجميع المهام اللازمة لضمان استمرارية العمل بالموقع .
- تلتزم إدارة تقنية المعلومات بتقديم التدريب اللازم لإدارة الموقع الإلكتروني (لأي جهة لديها موقع إلكتروني تحت مظلة البوابة)، حيث يتم التنسيق لذلك أو طلبه من خلال خطاب رسمي لإدارة تقنية المعلومات.
- يحق لكل عضو هيئة تدريس ومن في حكمه في الجامعة الحصول على التدريب اللازم لإدارة صفحته الشخصية تحت صفحات أعضاء هيئة التدريس.
- يحق لأعضاء هيئة التدريس ومن في حكمهم الحصول على التدريب اللازم لإدارة صفحاتهم الشخصية ضمن صفحات أعضاء هيئة التدريس أو مواقع الجهات وذلك بالتنسيق مع إدارة تقنية المعلومات بشكل مباشر.

8.2 السياسات المتعلقة بالشبكة الداخلية



- لا يسمح باستخدام اتصال VPN إلا عند الضرورة وللأشخاص المحددين وفقاً للتالي:
 - الشخص الذي لديه صلاحية تقديم الدعم التقني الطارئ على أحد الأنظمة الإلكترونية للجامعة.
 - مدير النظام الذي يحدده مالك الخدمة.
 - الموردون المعتمدين من إدارة تقنية المعلومات بعد التوريدات والتركيبات اللازمة.
- يتم طلب الخدمة وفقاً لمخطط سير العمل المحدد مسبقاً والمعتمد من عميد إدارة تقنية المعلومات.
- على إدارة تقنية المعلومات تشفير الحساب الشخصي المعتمد والمستخدم للاتصال بشبكة الجامعة من خلال خدمة SSL VPN أثناء العبور عبر شبكات غير مؤمنة وموثوق بها.
- يجب استيفاء متطلبات التعقيد والصعوبة الخاصة بكلمات المرور وفقاً لسياسة (user password management)
- يجب على الموظفين المصرح لهم من قبل الجامعة التأكد من ألا يتم السماح للمستخدمين الغير مصرح لهم بمشاركة خدمات الـ VPN الخاصة بالجامعة، أو الحصول على كلمة المرور الخاصة بهم، أو الوصول واستخدام جهاز الكمبيوتر أثناء عملية الاتصال.
- تأمين جميع أجهزة الكمبيوتر المتصلة بشبكة الجامعة من خلال خدمة الـ VPN وفقاً لمعايير إدارة تقنية المعلومات الخاصة بالبرامج المضادة للفيروسات بأحدث إصدارات للملفات الخاصة بها وكذلك آخر تحديث من تصحيحات الأمان الخاصة بنظام التشغيل.
- يمكن فقط استخدام تطبيقات الاتصال الخاصة بالكمبيوتر المعتمدة لفتح قنوات اتصال بشبكة الجامعة من خلال خدمة الـ VPN.
- سيتم قطع الاتصال تلقائياً عن الموظفين المصرح لهم بالدخول على شبكة الجامعة من خلال خدمة الـ VPN بعد ساعة واحدة من عدم النشاط.

- تخضع أجهزة الكمبيوتر للموظفين المصرح لهم بالدخول على الشبكة من خلال خدمة الـ VPN وفقاً لاحتياجات العمل الخاصة بهم لتقييد الوصول إلى الشبكة.
- على إدارة تقنية المعلومات فحص ورصد ومراجعة جميع قنوات اتصال الـ VPN بجامعة المستقبل.
- يمنع منح اتصال VPN إذا كان المستفيد خارج المملكة العربية السعودية إلا في حالات الضرورة، ولإدارة تقنية المعلومات الحق في الرفض أو السماح.
- لإدارة تقنية المعلومات الحق في المراقبة أو التحديد أو الفصل لأي اتصال VPN ولأي غرض دون إشعار مسبق.



3. سياسة خصوصية واستخدام البيانات بجامعة المستقبل

مقدمة

تعد جامعة المستقبل من الجامعات الرائدة في الجوانب التعليمية والبحثية والخدمة المجتمعية، وتتميز في تكوينها للبيئة العلمية الأكاديمية بأسسها وسياساتها التي تعزز تحقيق الرؤية الطموحة للمملكة. وترتكز في ذلك على النظم والتشريعات واللوائح المعمول بها، وتحقيق الامتثال الكامل لزراع الثقة لدى المستفيدين من خدماتها. وتولي الجامعة أهمية بالغة لحماية خصوصية البيانات الشخصية، وتلتزم بالامتثال الكامل لنظام حماية البيانات الشخصية ولوائح التنفيذ، وبما يحقق أعلى معايير الثقة والشفافية في تعاملها مع المستفيدين من خدماتها التعليمية والإدارية والبحثية والمجتمعية. وتهدف هذه السياسة إلى بيان كيفية جمع ومعالجة وحماية البيانات الشخصية التي تحصل عليها الجامعة بوسائلها المختلفة، سواء كانت مباشرة أو غير مباشرة، وذلك في إطار أداء مهامها واختصاصاتها النظامية، وبما يتوافق مع الأنظمة واللوائح ذات العلاقة المعمول بها في المملكة العربية السعودية.

1.3 الموافقة على سياسة الخصوصية

يعد استخدام موقع جامعة المستقبل إقرارًا بالاطلاع على سياسة الخصوصية، وقد تعتمد الجامعة في معالجة البيانات على مسوغات نظامية أخرى وفق ما ورد في هذه السياسة.

2.3 التغييرات على سياسة الخصوصية

تمتلك الجامعة حق إجراء أية تغييرات أو تعديلات على هذا الإشعار في أي وقت، وتصبح التعديلات سارية فور نشر الإشعار المحدث.

3.3 البيانات الشخصية التي يتم جمعها

تلتزم الجامعة بأن يقتصر جمع البيانات على الحد الأدنى اللازم، وتشمل:

1. البيانات الشخصية الأساسية

2. بيانات التواصل

3. البيانات الوظيفية

4. البيانات الأكاديمية

5. البيانات البحثية

6. البيانات المالية

7. البيانات الطبية والصحية

8. البيانات التعاقدية

4.3 طرق جمع البيانات الشخصية

تشمل:

1. الربط مع مزودي الخدمات الحكومية عبر النفاذ الوطني

2. البيانات التقنية عبر ملفات تعريف الارتباط

3. القنوات الرسمية للجامعة

5.3 أسباب جمع البيانات

أسباب جمع البيانات:

• التسجيل في الخدمات

• التقديم على القبول

• التقديم على الوظائف

• الالتحاق بالدورات

• الحصول على الخدمات الطبية

• استخدام الموقع بشكل فعال

6.3 كيفية استخدام البيانات

تشمل:

• الأعمال التنظيمية

• إتمام الطلبات

• التحليل والإحصاء

• الرسائل التوعوية

• قبول الطلاب ومتابعتهم

• الرد على الاستفسارات

• تحسين تجربة المستخدمين



7.3 مشاركة البيانات الشخصية

لا تتم مشاركة البيانات إلا بوجود مسوغ نظامي، وبالحد الأدنى اللازم، وفق نظام حماية البيانات الشخصية.

8.3 المسوغات النظامية

تشمل المسوغات النظامية:

1. نظام حماية البيانات الشخصية
2. اللائحة التنفيذية للنظام
3. سياسة مشاركة البيانات SDAIA –
4. موافقة المستخدم
5. الالتزامات التعاقدية
6. الالتزامات النظامية
7. تحقيق المصلحة العامة

9.3 تخزين البيانات وإتلافها

- تخزين البيانات داخل المملكة
- تطبيق أعلى معايير الأمن
- تتلف البيانات بعد انتهاء الغرض
- قد تمتد مدة الاحتفاظ في حالات نظامية أو قضائية

10.3 حقوق أصحاب البيانات

تشمل:

1. الحق في العلم
 2. الحق في الوصول للمعلومات
 3. الحق في الحصول على نسخة
 4. الحق في التصحيح
 5. الحق في الإتلاف
- ويتم الرد خلال 30 يومًا من استلام الطلب.

11.3 بيانات التواصل

مسؤول حماية البيانات الشخصية VP-PGR@uom.edu.sa

في حال عدم الرضا يمكن تقديم شكوى إلى:

• الهيئة السعودية للبيانات والذكاء الاصطناعي SDAIA

• منصة حوكمة البيانات الوطنية DGP



خاتمة

يمثل هذا الدليل إطاراً تنظيمياً شاملاً يهدف إلى تعزيز حوكمة المعلومات داخل جامعة المستقبل، وضمان التعامل السليم مع البيانات بمختلف أنواعها، سواء في مراحل الحفظ أو التداول أو النشر أو الاستخدام التقني. وتؤكد الجامعة التزامها الكامل بتطبيق السياسات والإجراءات الواردة في هذا الدليل، وبما يتوافق مع الأنظمة الوطنية ذات العلاقة، وفي مقدمتها نظام حماية البيانات الشخصية، وسياسات الأمن السيبراني، وضوابط مشاركة البيانات.

وتدعو الجامعة جميع منسوبيها من أعضاء هيئة التدريس والموظفين والطلاب إلى الالتزام بما ورد في هذا الدليل، والعمل بروح المسؤولية لضمان حماية المعلومات وصون خصوصية الأفراد، وتعزيز الثقة في البيئة الرقمية للجامعة. كما ستعمل الجامعة على مراجعة هذا الدليل وتحديثه بشكل دوري لمواكبة التطورات التقنية والتنظيمية، وضمان استمرار توافقه مع أفضل الممارسات والمعايير المعتمدة.