مكتب إدارة البيانات
Data Management Office

سياسات حوكمة البيانات
بجامعة الملك عبدالعزيز

الإصـدار الثـاني
فبراير ٢٠٢٥ م

المحتويات

المحتوى	الصفحة
مقدمة	3
التعريفات	4
ملكية سياسات حوكمة البيانات	6
الامتثال لهذه السياسات	6
الأهداف	7
1- سياسة تصنيف البيانات	8
2- سياسة حماية البيانات الشخصية	17
3- سياسة مشاركة البيانات	23
4- سياسة حرية المعلومات	30
5- سياسة البيانات المفتوحة	34
6- سياسة حماية البيانات الشخصية للأطفال ومن في حكمهم	37
7- القواعد العامة لنقل البيانات الشخصية خارج الحدود الجغرافية للمملكة العربية السعودية	43

مقدمة

تعد البيانات أحد الأصول الاستراتيجية الأساسية التي تعتمد عليها المؤسسات لتحقيق أهدافها وتعزيز كفاءتها. وفي جامعة الملك عبدالعزيز، ندرك أهمية البيانات في دعم مسيرتنا نحو الابتكار الأكاديمي والبحثي والإداري، وتعزيز مكانتنا كمؤسسة تعليمية رائدة.

يهدف هذا الملف إلى توضيح السياسات والإجراءات المتعلقة بحوكمة البيانات وإدارتها بالجامعة، بما يضمن الالتزام بالمعايير الوطنية والدولية، والحفاظ على الخصوصية والسرية، وتعزيز ثقافة الشفافية والمشاركة، كما يعكس هذا الملف التزام الجامعة بتحقيق أعلى مستويات الجودة في حوكمة البيانات بما يتماشى مع سياسات مكتب إدارة البيانات الوطنية، ويدعم جهود الجامعة في تحقيق التكامل والتطوير المستدام.

إن هذه السياسات تمثل إطارًا تنظيميًا يساعد في إدارة البيانات بفعالية، ويضمن استخدامًا مسؤولاً وأخلاقيًا لها، مع التركيز على حماية حقوق الأفراد وتعزيز الشفافية والابتكار لخدمة المجتمع والعملية التعليمية.

التعريفات

سعيـًا لتطبيق هذه السياسات، تم تحديد معاني الكلمات والمصطلحات الرئيسة الواردة فيها، وتعني أينما وردت المعاني الموضحة أمامها، ما لم يقتض سياق النص خلاف ذلك، وهي:

1. **الجامعة:** جامعة الملك عبدالعزيز.
2. **المكتب:** مكتب إدارة البيانات بجامعة الملك عبدالعزيز.
3. **البيانات:** مجموعة من الحقائق في صورتها الأولية أو في صورة غير منظمة مثل الأرقام أو الحروف أو الصور الثابتة أو التسجيلات المرئية أو التسجيلات الصوتية أو الرموز التعبيرية.
4. **إدارة البيانات:** عملية تطوير وتنفيذ الخطط والسياسات والبرامج والممارسات والإشراف عليها لتمكين حوكمة البيانات وتعزيز قيمتها باعتبارها أحد الأصول الإستراتيجية.
5. **الضوابط:** هي مجموعة من المبادئ والقواعد والتوجيهات التي تُمكن المنظمة من الوصول إلى أهدافها بعيدة المدى.
6. **مستويات تصنيف البيانات:** مستويات التصنيف المعتمدة من مكتب إدارة البيانات الوطنية، وهي: "سري للغاية"، " سري"، "مقيد"، "عام".
7. **الوصول الى البيانات:** القدرة على الوصول المنطقي والمادي إلى البيانات لغرض استخدامها.
8. **سرية البيانات:** الحفاظ على القيود المصرح بها للوصول إلى البيانات او الإفصاح عنها.
9. **البيانات الشخصية:** كل بيان - مهما كان مصدره أو شكله – من شأنه أن يؤدي إلى معرفة الفرد على وجه التحديد، أو يجعله قابلاً للتعرف عليه بصفةٍ مباشرة أو غير مباشرة عند دمجه مع بيانات أخرى، ويشمل ذلك- على سبيل المثال لا الحصر – الاسم، وأرقام الهويات الشخصية، والعناوين، وأرقام التواصل، وأرقام الحسابات البنكية والبطاقات الائتمانية، وصور الفرد، وغير ذلك من البيانات ذات الطابع الشخصي.
10. **صاحب البيانات الشخصية:** الشخص الطبيعي الذي تتعلق به البيانات الشخصية أو من يمثله أو من له الولاية الشرعية عليه.
11. **الامتثال:** تطبيق بنود هذه السياسة وضمان المراقبة الدورية لذلك.
12. **المصدر الموثوق:** مصدر مرجعي للبيانات تم إثبات موثوقيته من خلال التحقق المسبق من صحته.
13. **التفويض:** عملية يجري من خلالها منح طرف آخر صلاحيات التصرف للقيام بأنشطة معينة خلال فترة محددة مع بقاء المسؤولية على الشخص المفوض.

14. **معالجة البيانات:** عملية تجري على البيانات بأحد الوسائل اليدوية أو الآلية، ومن ذلك عمليات الجمع والتسجيل والحفظ والفهرسة والترتيب والتنسيق والتخزين والتعديل والتحديث والدمج والاسترجاع والاستعمال والإفصاح والنقل والنشر والمشاركة والحجب والمسح والإتلاف.

15. **بيانات غير معالجة:** البيانات التي لم تخضع للمعالجة أو للتبادل بصورة أولية بأي صيغةٍ كانت.

16. **البيانات الحساسة:** البيانات التي يؤدي فقدانها أو إساءة استخدامها أو الوصول غير المصرح به إليها أو تعديلها إلى ضرر جسيم أو تأثير سلبي على المصالح الوطنية أو أنشطة الجهات الحكومية أو خصوصية الأفراد وحماية حقوقهم.

17. **مستخدم البيانات:** أي شخص يمنح صلاحية الوصول إلى البيانات؛ لغرض الاطلاع عليها أو استخدامها أو تحديثها وفق المهام المصرح بها.

18. **الضوابط الأمنية:** الأجهزة والإجراءات والسياسات والضمانات المادية المستخدمة لضمان سلامة البيانات وحمايتها ومعالجتها والوصول إليها.

19. **الإفصاح:** تمكين أي شخص - عدا جهة التحكم أو جهة المعالجة بحسب الأحوال - من الحصول على البيانات الشخصية أو استعمالها أو الاطلاع عليها بأي وسيلة ولأي غرض.

20. **سياسة الخصوصية:** هي وثيقة داخلية موجهة إلى العاملين في الجهة توضح حقوق أصحاب البيانات والالتزامات التي يجب الامتثال لها؛ للمحافظة على خصوصية أصحاب البيانات وحماية حقوقهم.

21. **الصلاحيات:** عملية إعطاء الأفراد أو الجهات قدرات أوسع أو (سلطة) لممارسة التحكم وتحمل المسؤولية عن مهام محددة.

22. **الإجراءات:** يقصد بها تصميم خطوات العمل في الجهة وتوثيقها بحيث تتم بتسلسل واضح حسب الأنظمة واللوائح والمسؤوليات الموجودة في الهيكل التنظيمي لضمان الكفاءة المناسبة التي تخدم توجه الجهة في تحسين العمليات وتقديم الخدمات.

23. **السياسة:** وثيقة تنظيمية تقوم بتحديد السياق أو طريقة العمل لإرشاد وتحديد الخطوات الحالية والمستقبلية، كما تحدد المطلوب من الجهات داخل الجامعة أو خارجها من خلال المبادئ التي تضمنتها السياسات.

24. **التشفير:** تحويل البيانات من تنسيق قابل للقراءة إلى تنسيق مشفر. لا يمكن قراءة البيانات المشفرة أو معالجتها إلا بعد فك تشفيرها.

25. **هيكلة البيانات:** طريقة لتنظيم البيانات وتخزينها في ذاكرة الحاسب للوصول إليها ومعالجتها بكفاءة.

26. **الطفل:** كل شخص لم يتجاوز الثامنة عشرة من عمره.

27. **ولي أمر الطفل/ولي الطفل:** أحد الوالدين أو من تكون له الولاية على شؤون الطفل حسب أحكام الشريعة أو الأنظمة ذات العلاقة.

ملكية سياسات حوكمة البيانات

تعود ملكية سياسات حوكمة البيانات لمكتب إدارة البيانات في جامعة الملك عبدالعزيز، وإصدار النسخ المحدثة منها.

الامتثال لهذه السياسات

يجب على جميع منسوبي الجامعة والمتعاقدين معها الالتزام بهذه السياسات، وعلى جهات الجامعة ضمان تطبيق هذه السياسات داخل إداراتها، علمًا بأن الالتزام ببنود هذه السياسات يخضع لمراجعة دورية من مكتب إدارة البيانات بالجامعة، وأي عدم التزام أو انتهاك لها سيؤدي إلى المساءلة القانونية واتخاذ الإجراءات اللازمة حسب ما يوصي به مكتب إدارة البيانات بالجامعة.

الأهداف

تهدف هذه السياسات إلى تبني أفضل الممارسات والمعايير العالمية في مجال حوكمة البيانات، بما يتماشى مع سياسات وضوابط مكتب إدارة البيانات الوطنية، لتحقيق الأهداف التالية:

1. المساهمة في تحقيق رؤية المملكة 2030 وتعزيز الاستراتيجيات الوطنية من خلال تحسين إدارة البيانات ودعم التحول الرقمي لتحقيق التنمية المستدامة.
2. تعزيز ثقافة إدارة ومشاركة البيانات داخل الجامعة لدعم تكامل العمليات وتطوير الأصول المعرفية بما يرفع من كفاءة العمل المؤسسي.
3. تنظيم جمع البيانات وتصنيفها وتبادلها بما يضمن حماية الحقوق والامتثال للضوابط الوطنية المتعلقة بحوكمة البيانات.
4. دعم الأبحاث والابتكار من خلال توفير بيانات دقيقة وآمنة تسهم في تطوير البحث العلمي وتعزيز التنمية الاقتصادية والاجتماعية.
5. تعزيز الشفافية والمسؤولية عبر وضع سياسات واجراءات واضحة لتوزيع الأدوار والمسؤوليات المتعلقة بإدارة البيانات.
6. حماية خصوصية البيانات الشخصية وسرية البيانات الحساسة وفقًا للأنظمة الوطنية، مع ضمان السيادة الرقمية للجامعة.
7. رفع مستوى الخدمات الأكاديمية والإدارية الإلكترونية من خلال تحسين جودة البيانات وضمان تكاملية النظم المستخدمة.
8. تمكين اتخاذ القرارات المستندة إلى البيانات من خلال توفير معلومات موثوقة ودقيقة للإدارة العليا والقطاعات المختلفة بالجامعة.
9. إتاحة المعلومات العامة وفق السياسات الوطنية لدعم الشفافية وتوفير فرص متكافئة لجميع الأطراف المهتمة.
10. تعزيز ثقافة التعامل الأمثل مع البيانات عبر سياسات تلزم الأطراف المعنية بتطبيق أفضل الممارسات وضمان الامتثال.

1

سياسة تصنيف البيانات

1.1 النطاق

تنطبق أحكام هذه السياسة على جميع البيانات التي تتلقاها أو تنتجها أو تتعامل معها جامعة الملك عبدالعزيز- سواء أكانت أنتجت أم استخدمت قبل اعتماد هذه السياسة أم بعدها - مهما كان مصدرها، أو شكلها أو طبيعتها، ويشمل ذلك السجلات الورقية، الاجتماعات، والاتصالات عبر وسائل التواصل والتطبيقات، ورسائل البريد الإلكتروني، والبيانات المخزنة على وسائط إلكترونية، وأشرطة الصوت أو الفيديو، والخرائط، والصور الفوتوغرافية، والمخطوطات، والوثائق المكتوبة بخط اليد، وأي شكل آخر من أشكال البيانات المسجلة.

1.2 المبادئ الرئيسية لتصنيف البيانات

يتم تصنيف البيانات وفق المبادئ الرئيسية التالية:

المبدأ الأول: الأصل في البيانات الإتاحة

الأصل في البيانات أن تكون متاحة "عامة" ما لم تقتضي طبيعتها أو حساسيتها مستويات أعلى من التصنيف والحماية.

المبدأ الثاني: الضرورة والتناسب

يتم تصنيف البيانات بما يتناسب مع طبيعتها ومستوى حساسيتها، مع الأخذ بعين الاعتبار الأهمية للبيانات والحاجة إلى حمايتها من ثم الموازنة بين قيمتها ودرجة سريتها.

المبدأ الثالث: التصنيف في الوقت المناسب

يتم تصنيف البيانات عند إنشائها أو حين تلقيها من جهات أخرى ويكون التصنيف خلال فترة زمنية محددة. وذلك لضمان معالجتها وحمايتها بشكل مناسب منذ البداية.

المبدأ الرابع: المستوى الأعلى من الحماية

في حال تضمين مجموعة من البيانات مستويات مختلفة من التصنيف، يتم اعتماد مستوى التصنيف الأعلى لضمان الحماية الكاملة لجميع البيانات ذات الصلة.

المبدأ الخامس: فصل المهام

يتكفل مكتب إدارة البيانات بالجامعة بالمهام والمسؤوليات حصريًا فيما يتعلق بتصنيف البيانات أو الوصول إليها أو الإفصاح عنها أو استخدامها أو التعديل عليها أو إتلافها ولا يحق لأي جهة من جهات الجامعة القيام بها أو عدم الخضوع لها.

المبدأ السادس: الحاجة إلى المعرفة

يتم تقييد الوصول إلى البيانات واستخدامها على أساس الاحتياج الفعلي للمعرفة، بحيث تمنح الصلاحيات لمنسوبي الجامعة في الوصول للبيانات بقدر حاجة مهامهم الوظيفية لذلك.

المبدأ السابع: الحد الأدنى من الامتيازات

يتم تقييد إدارة صلاحيات الوصول على الحد الأدنى من الامتيازات اللازمة لأداء المهام والمسؤوليات المناط به للمنسوبين.

هذه المبادئ تضمن تطبيق سياسة تصنيف البيانات بطريقة تراعي الاحتياجات الخاصة للبيئة الأكاديمية والإدارية للجامعة، مع الحفاظ على الأمان والخصوصية لجميع البيانات ذات الصلة.

1.3 مستويات تصنيف البيانات

يتم تصنيف البيانات إلى أحد المستويات التالية: **سري للغاية، سري، مقيد ،عام.** يوضح الجدول التالي مستويات التصنيف بناءً على الأثر.

مستوى التصنيف	درجة الأثر	الوصف	أمثلة استرشادية
سري للغاية	عالي	البيانات التي تصنف على أنها "**سري للغاية**" هي تلك التي تحتوي على معلومات حساسة جدًا، والتي إذا تم الوصول إليها أو الكشف عنها بطريقة غير مصرح بها، يمكن أن تؤدي إلى أضرار جسيمة وغير قابلة للإصلاح بالنسبة للأمن والسمعة والوضع التشغيلي للجامعة والمصالح الوطنية والشؤون المتعلقة بالتعليم والبحث العلمي. هذه الفئة من البيانات تتطلب أعلى درجات السرية والحماية نظرًا للعواقب الوخيمة المحتملة على الجامعة والأفراد المرتبطين بها في حالة إساءة استخدامها أو تسريبها.	• بيانات حول البحوث السرية أو غير المنشورة التي تحمل القدرة على إحداث تغيير كبير في مجال معين. • تفاصيل حول التقنيات الناشئة أو الملكية الفكرية التي لم يتم توثيقها بعد والتي يمكن أن تعطي ميزة تنافسية كبيرة. • السجلات المتعلقة بالموظفين أو الطلاب التي تحتوي على معلومات شخصية حساسة مثل السجلات الطبية أو المعلومات المالية. • تفاصيل البروتوكولات الأمنية الخاصة بالحرم الجامعي، بما في ذلك أنظمة المراقبة وإجراءات الاستجابة للحوادث. • تفاصيل حول بنية تقنية المعلومات والاتصالات الحساسة وأنظمة الشبكات التي تدعم عمليات الجامعة الحيوية. • مستندات تحتوي على قرارات إدارية كبرى، مثل التعيينات الجديدة أو الخطط الاستراتيجية. هذه الأمثلة تعكس نوعية البيانات التي يجب أن تعالج بأقصى درجات الحذر والسرية في الجامعة، ويجب حمايتها من أي وصول غير مصرح به لضمان الحفاظ على سلامة وأمان الجامعة ومجتمعها.

مستوى التصنيف	درجة الأثر	الوصف	أمثلة استرشادية
سري	متوسط	مستوى التصنيف "**سري**" يشمل البيانات التي تعتبر حساسة والتي يمكن أن يؤدي الوصول غير المصرح به إليها أو الإفصاح عنها إلى ضرر ملموس لكن يمكن تداركه على الوضع التشغيلي، السمعة، أو الأصول للجامعة. هذه البيانات تتطلب إجراءات حماية مهمة لكنها لا تحتاج إلى مستوى الحماية الشديد الذي تتطلبه البيانات المصنفة كـ"سري للغاية". يتوقع أن يكون الوصول إليها محدودا لأفراد معينين ضمن الجامعة ويطلب منهم التعامل مع هذه البيانات بمسؤولية وسرية.	• تقارير حول تقييم البرامج أو تقييمات الأقسام التي تحلل الأداء والتي قد تؤثر على سمعة الجامعة. • تفاصيل حول المنح البحثية الجديدة أو التمويلات التي لم يتم الإعلان عنها بعد، والتي يمكن أن تعطي الجامعة ميزة تنافسية. • الدرجات الطلابية والسجلات الأكاديمية التي لم يتم إتاحتها علنا، والتي تحتوي على معلومات شخصية وأكاديمية حساسة. • مراسلات بين أعضاء الهيئة الإدارية تتضمن مناقشات حول تغييرات سياسات الجامعة أو قرارات مهمة تؤثر على العمليات الداخلية. • معلومات مفصلة حول الميزانيات، والتخطيط المالي، والتي يمكن أن تؤثر على العمليات التشغيلية والمالية للجامعة. • بيانات حول برامج التطوير التي لم يتم الإعلان عنها، والتي قد تؤثر على المسارات المهنية للمعنيين. كل هذه الأمثلة تتطلب مستوى عال من الحماية لضمان عدم تسريب المعلومات الحساسة التي قد تؤثر سلبًا على الجامعة إذا تم الكشف عنها دون تخطيط.
مقيد	منخفض	مستوى التصنيف "**مقيد**" يشير إلى البيانات التي تكون حساسة لكنها ليست بالدرجة العالية من الحساسية كما في المستويات "سري للغاية" أو "سري". الوصول غير المصرح به إلى هذه البيانات أو الإفصاح عنها قد يؤدي إلى ضرر محدود قد يؤثر على العمليات الداخلية للجامعة أو على الخصوصية الشخصية، لكنه لا يصل إلى مستوى الضرر الجسيم الذي يتطلب مستويات التصنيف الأعلى.	• جداول العمل الخاصة بالموظفين، تقارير الحضور والغياب، ومعلومات الجدولة الدورية للمحاضرات والفعاليات الجامعية. • الاتصالات اليومية بين الأقسام والمراسلات التي لا تحتوي على معلومات استراتيجية، مثل الإشعارات الداخلية والتحديثات الإدارية. • تقارير المصروفات والميزانيات التشغيلية الصغيرة التي لا تحتوي على بيانات شديدة الحساسية.

مستوى التصنيف	درجة الأثر	الوصف	أمثلة استرشادية
مقيد	منخفض	هذه الفئة من البيانات تتطلب تدابير حماية لضمان الخصوصية والأمان، لكن متطلبات الحماية ليست بالغة كما في الفئات الأعلى من التصنيفات. يعتبر التعامل مع هذه البيانات جزءا من إجراءات الحفاظ على السرية الروتينية في الجامعة.	• توزيعات الدرجات والتقييمات الفردية للطلاب التي يتم التعامل معها ضمن الأقسام الأكاديمية. • البيانات الأولية للأبحاث التي لا تحمل قيمة استراتيجية كبيرة أو لم تتم مراجعتها بعد لنشرها. كل هذه الأمثلة تعتبر حساسة وتتطلب مستوى من الحماية لضمان الخصوصية ومنع الإفصاح، ولكنها لا تصل إلى درجة الحماية الشديدة اللازمة للبيانات ذات التصنيف الأعلى. يتوجب تقييد وصول الأشخاص إلى هذه البيانات بناءً على الحاجة إلى المعرفة والدور الوظيفي.
عام	لا يوجد	مستوى التصنيف "**عام**" يطبق على البيانات التي لا تعتبر حساسة ويمكن مشاركتها مع العامة دون أن يسبب ذلك ضررًا للمصالح الجامعية أو الفردية. هذه البيانات عادةً ما تكون معلومات مصممة للنشر العام ولا تتطلب إجراءات حماية مشددة. هذه الفئة من البيانات لا تتطلب تدابير حماية خاصة وعادةً ما تكون متاحة بشكل عام على الموقع الإلكتروني للجامعة أو من خلال المنشورات والوسائل الإعلامية الأخرى.	• كتيبات الجامعة، الخرائط، معلومات عن المرافق والخدمات الطلابية التي تقدم للعموم. • تقويم الأحداث الجامعية الذي يعلن عن الندوات، الفعاليات والأنشطة. • الأوراق البحثية والمقالات التي تم نشرها وهي متاحة للعامة. • اللوائح الأكاديمية وسياسات الجامعة. • الخدمات التي تقدمها الجامعة للمجتمع، مثل العيادات الصحية أو المراكز الاستشارية. هذه الأمثلة تظهر نوعية المعلومات التي يمكن مشاركتها بحرية مع الجمهور العام دون الحاجة إلى تدابير أمنية مشددة، حيث إنها تصمم للنشر ولا تحمل مخاطر أمنية.

جدول 1 مستويات تصنيف البيانات

1.4 ضوابط تصنيف البيانات

الضابط الأول: البيانات غير المصنفة

- تعامل هذه البيانات على أنها "مقيدة" حتى يتم تصنيفها بشكل صحيح.
- يتم تصنيف البيانات التي لم يتم تصنيفها خلال فترة زمنية محددة بموجب خطة عمل يعدها مكتب إدارة البيانات.

الضابط الثاني: علامات الحماية

- تطبق علامات الحماية النصية على الوثائق الورقية والإلكترونية بما فيها رسائل البريد الإلكتروني وفقًا لمستويات التصنيف.
- تتضمن علامات الحماية اسم التصنيف (عام، مقيد، سري، سري للغاية) وتاريخ انتهاء التصنيف، وتطبق على كل الصفحات، بما في ذلك الصفحة الأولى.

الضابط الثالث: حق الوصول

- يمنح الوصول (المنطقي والمادي) للبيانات بناءً على مبدأ "الحد الأدنى من الامتيازات" و "الحاجة إلى المعرفة".
- يمنع الوصول إلى البيانات بمجرد انتهاء أو إنهاء الخدمة المهنية للمنسوب بالجامعة.

الضابط الرابع: الاستخدام

- تستخدم البيانات المصنفة وفقًا لمتطلبات مستويات التصنيف، على سبيل المثال، يتم تقييد استخدام البيانات المصنفة "سرية للغاية" على مواقع محددة سواء مادية – كالمكاتب – أو افتراضية باستخدام ترميز الأجهزة أو تطبيقات خاصة.

الضابط الخامس: التخزين

- تكون البيانات المصنفة على أنها "سري للغاية" و "سري" و "مقيد" وكذلك الأجهزة المحمولة التي تعالج أو تخزن هذه البيانات تحت المراقبة بشكل دائم.
- تتم حماية البيانات المصنفة على أنها "سري للغاية" و "سري" و "مقيد" غير المراقبة أثناء تخزينها ماديًا أو إلكترونيًا باستخدام أحد طرق التشفير المعتمدة من قبل الهيئة الوطنية للأمن السيبراني.

الضابط السادس: مشاركة البيانات

- يتم تحديد الوسائل المادية والرقمية المناسبة لتبادل البيانات بشكل آمن بما يضمن تقليل المخاطر المحتملة والامتثال لأنظمة وسياسات مشاركة البيانات وآلية تبادل البيانات.
- يتم التحقق من مستوى تصنيف البيانات قبل مشاركتها داخليًا أو خارجيًا.

الضابط السابع: الاحتفاظ بالبيانات

- يتم إعداد جدول زمني يحدد فترة الاحتفاظ بجميع البيانات.
- يتم تحديد فترة الاحتفاظ بالبيانات بناء على ما تحدده المتطلبات الإدارية والتشغيلية والتعاقدية والتنظيمية والقانونية ذات العلاقة.
- يتم مراجعة الجدول الزمني لفترة الاحتفاظ بالبيانات بشكل دوري - سنوي أو إذا طرأت تغييرات على المتطلبات ذات العلاقة.

الضابط الثامن: التخلص من البيانات

- يتم التخلص من جميع البيانات بشكل آمن وفقًا للجدول الزمني للاحتفاظ بالبيانات بعد الحصول على موافقة رئيس قسم حوكمة وحماية البيانات.
- يتم التخلص من البيانات التي تم تصنيفها على أنها "سري للغاية" و "سري" التي يتم التحكم بها إلكترونيًا باستخدام أحدث طرق التخلص من الوسائط الإلكترونية.
- يتم التخلص من جميع الوثائق الورقية باستخدام آلة تمزيق الورق.
- يتم إعداد سجل مفصل عن جميع البيانات التي تم التخلص منها.

الضابط التاسع: الأرشفة

- تتم أرشفة البيانات في مواقع تخزين آمنة وفقًا للطريقة التي يوصي بها مكتب إدارة البيانات، ويتم الاحتفاظ بنسخ احتياطية من البيانات المؤرشفة.
- تتم حماية البيانات المؤرشفة التي تم تصنيفها على أنها "سري للغاية" و "سري" باستخدام إحدى طرق التشفير المعتمدة من قبل الهيئة الوطنية للأمن السيبراني.
- يتم إعداد وتوثيق قائمة مفصلة تتضمن المستخدمين المصرح لهم بالوصول إلى البيانات المؤرشفة.

الضابط العاشر: إلغاء التصنيف (رفع السرية)

- يتم إلغاء تصنيف البيانات أو خفض مستوى تصنيفها إلى الحد المناسب بعد انتهاء مدة التصنيف عندما لا تكون الحماية مطلوبة أو أنها لم تعد مطلوبة على المستوى الأصلي للتصنيف.
- في حال تم تصنيف البيانات بشكلٍ خاطئ، يتم تحديد مدى الحاجة إلى إعادة تصنيفها بشكل مناسب.
- يتم تحديد عوامل إلغاء تصنيف البيانات عند تحديد مستويات التصنيف لأول مرة، وتسجيلها في سجل أصول البيانات.
- يتم دراسة طلب إلغاء التصنيف (رفع السرية) أو خفض مستويات التصنيف جيدًا ليُكوّن فهمًا سليمًا لمحتوى البيانات السرية والسياق الذي وردت فيه.
- يتم الحصول على موافقة رئيس قسم حوكمة وحماية البيانات لإلغاء التصنيف أو خفضه.

1.5 الأدوار والمسؤوليات

يتولى مكتب إدارة البيانات بجامعة الملك عبدالعزيز مسؤولية الإشراف وتنفيذ كافة المهام المتعلقة بتصنيف البيانات، بما يضمن الالتزام بالسياسات والإجراءات المعتمدة من مكتب إدارة البيانات الوطنية. ويعمل المكتب على توجيه عمليات تصنيف البيانات والإشراف عليها لضمان توافقها مع اللوائح الوطنية ومتطلبات الجامعة، مع تحقيق التوازن بين حماية البيانات وإتاحتها بما يخدم أهداف الجامعة الأكاديمية والإدارية. كما يُناط بمدير مكتب إدارة البيانات مراجعة واعتماد مستويات التصنيف بما يتماشى مع أفضل الممارسات والمعايير الوطنية.

وتأتي أدوار ومسؤوليات المكتب فيما يلي:

- **إعداد السياسات والإجراءات:**

  يتولى مكتب إدارة البيانات إعداد وتطوير سياسات وإجراءات تصنيف البيانات بما يتماشى مع المعايير الوطنية والدولية، ويعمل على تحديثها بشكل دوري لضمان مواكبتها للتطورات التقنية والقانونية.

- **تصنيف البيانات:**

  يعمل المكتب على تصنيف البيانات التي تجمعها الجامعة أو الجهات التابعة لها وفقـًا للسياسات والاجراءات المعتمدة في هذه السياسة.

- **مواءمة تصنيف البيانات:**

  يتولى المكتب مسؤولية التأكد من تصنيف البيانات المجمعة من مصادر متعددة بدقة، مع ضمان حماية البيانات وفقـًا لأعلى مستوى من السرية المطلوبة لأي جزءٍ منها.

- **المراجعة والإشراف:**

  يقوم المكتب بمراجعة عمليات تصنيف البيانات بشكل دوري للتأكد من الالتزام بالضوابط والمعايير المعتمدة، مع الإشراف على تنفيذ مهام التصنيف لجميع البيانات التي تتعامل معها الجامعة.

- **إدارة أصول البيانات:**

  يتولى المكتب مسؤولية تسجيل جميع أصول البيانات الخاصة بالجامعة وتصنيفها وفق السياسات المعتمدة، مع التأكد من توثيق عمليات التصنيف في السجلات الرسمية.

- **معالجة الاستثناءات:**

  يتولى المكتب مسؤولية مراجعة طلبات الاستثناء المتعلقة بتصنيف البيانات، مثل طلبات رفع أو خفض مستوى التصنيف، واتخاذ القرارات المناسبة بالتنسيق مع الجهات ذات العلاقة.

- **التنسيق مع الجهات الداخلية والخارجية:**

  يعمل المكتب كجهة تنسيقية لضمان الالتزام بتصنيفات البيانات عند التعامل مع الجهات الخارجية أو الداخلية، وضمان التوافق مع الأنظمة الوطنية المتعلقة بتصنيف البيانات.

- **إعطاء الصلاحيات:**

يمنح المكتب الصلاحيات وفق مبدأ "الحاجة إلى المعرفة" بحسب تصنيف البيانات، بحيث يقتصر الوصول إلى البيانات على الأشخاص الذين تتطلب مهامهم الوظيفية ذلك.

- **مراجعة الصلاحيات:**

يقوم المكتب بمراجعة وتحديث صلاحيات الوصول بشكل دوري أو عند حدوث تغييرات في المناصب الوظيفية لضمان توافقها مع المتطلبات الوظيفية وتصنيف البيانات

- **التحكم في الوصول:**

التأكد من تطبيق ضوابط التحكم في الوصول ورصدها ومراجعتها وفقًا لمستويات تصنيف البيانات.

- **نشاط المراقبة:**

يقوم المكتب بمراقبة الأنشطة التي تتم على البيانات وتسجيلها لضمان توافق الاستخدام مع مستوى التصنيف الخاص بالبيانات المستخدمة، بما في ذلك بيانات المستخدم.

- **التعامل مع الانتهاكات:**

يتولى المكتب مسؤولية التحقيق مع البلاغات عن أي انتهاكات لسياسات تصنيف البيانات، واتخاذ الإجراءات التصحيحية لذلك بالتنسيق مع الإدارات المعنية.

- **متابعة التنفيذ والتطوير:**

يضمن المكتب متابعة تنفيذ السياسة بجميع مراحلها وتطوير أدوات تقنية داعمة تسهم في تحسين عمليات التصنيف وضمان دقتها.

2

سياسة حماية البيانات الشخصية

2.1 النطاق

تنطبق أحكام هذه السياسة على جميع البيانات الشخصية التي تتلقاها أو تنتجها أو تتعامل معها جامعة الملك عبدالعزيز- سواءً أكانت أنتجت أم استخدمت قبل اعتماد هذه السياسة أو بعدها - مهما كان مصدرها، أو شكلها أو طبيعتها، ويشمل ذلك جميع أشكال البيانات الشخصية المتعلقة بالأفراد.

يُستثنى من نطاق تطبيق هذه السياسة في الأحوال التالية:

- إذا كان جمع البيانات الشخصية أو معالجتها مطلوبًا لتحقيق متطلبات نظامية وفقًا للأنظمة واللوائح والسياسات المعمول بها في المملكة العربية السعودية أو لاستيفاء متطلبات قضائية أو لتنفيذ التزام بموجب اتفاق تكون المملكة طرفًا فيه.
- إذا كان جمع البيانات الشخصية أو معالجتها ضروريًا لحماية الصحة أو السلامة العامة أو حماية المصالح الحيوية للأفراد.

2.2 المبادئ الرئيسية لحماية البيانات الشخصية

من أجل حماية البيانات الشخصية تلتزم الجامعة بالمبادئ الرئيسية التالية:

المبدأ الأول: المسؤولية

ضمان توفير السياسات والإجراءات لحماية البيانات الشخصية يعتبر جزءًا أساسيًا من مسؤولية مكتب إدارة البيانات، وهذا يشمل تطبيق المعايير والإجراءات بفعالية وتعزيز ثقافة الوعي بأهمية حماية البيانات الشخصية، بالإضافة إلى التأكد من توافق الإجراءات مع اللوائح المتعلقة بحماية البيانات الشخصية.

المبدأ الثاني: الشفافية

تتمثل الشفافية في حماية البيانات الشخصية في الوضوح والصراحة في جميع جوانب جمع، معالجة، ومشاركة هذه البيانات. هذا يعني توفير معلومات واضحة ومفهومة لأصحاب البيانات حول كيفية جمع البيانات الخاصة بهم وأسباب جمعها وطرق استخدامها ومعالجتها.

المبدأ الثالث: الاختيار والموافقة

ضمان أن الأفراد لديهم القدرة على اتخاذ القرار بشأن جمع واستخدام بياناتهم الشخصية وذلك بتوفير جميع المعلومات اللازمة بشكل واضح لفهم كيف ستستخدم بياناتهم، والسماح لهم بالموافقة على ذلك أو رفضه.

المبدأ الرابع: الحد من جمع البيانات

اقتصار جمع البيانات الشخصية على الحد الأدنى من البيانات الذي يمكن من تحقيق الأغراض المحددة في إشعار الخصوصية.

المبدأ الخامس: الحد من استخدام البيانات والاحتفاظ بها والتخلص منها

تقييد معالجة البيانات الشخصية بالأغراض المحددة في إشعار الخصوصية والتي من أجلها قدم صاحب البيانات موافقته الضمنية أو الصريحة، والاحتفاظ بها طالما كان ذلك ضروريًا لتحقيق الأغراض المحددة أو لما تقتضيه الأنظمة واللوائح والسياسات المعمول بها في المملكة وإتلافها بطريقة آمنة تمنع التسرب، أو الفقدان، أو الاختلاس، أو إساءة الاستخدام، أو الوصول الغير مصرح به نظامـًا.

المبدأ السادس: الوصول إلى البيانات الشخصية

توفير الوسائل التي عن طريقها يمكن لصاحب البيانات الوصول إلى بياناته الشخصية لمراجعتها، أو تحديثها، أو تصحيحها.

المبدأ السابع: الحد من الإفصاح عن البيانات

تقييد الإفصاح عن البيانات الشخصية للأطراف الخارجية بالأغراض المحددة في إشعار الخصوصية والتي من أجلها قدم صاحب البيانات موافقته الضمنية أو الصريحة.

المبدأ الثامن: أمن البيانات الشخصية

حماية البيانات من التسرب أو التلف أو الفقدان أو إساءة الاستخدام أو التعديل أو الوصول غير المصرح به – وفقـًا لما يصدر من الهيئة الوطنية للأمن السيبراني والجهات ذات الاختصاص.

المبدأ التاسع: جودة البيانات الشخصية

الاحتفاظ بالبيانات الشخصية بصورة دقيقة وكاملة وذات علاقة مباشرة بالأغراض المحددة في إشعار الخصوصية.

المبدأ العاشر: المراقبة والامتثال

مراقبة الامتثال لسياسات وإجراءات الخصوصية بالجامعة، ومعالجة الاستفسارات والشكاوى والنزاعات المتعلقة بالخصوصية.

2.3 الأدوار والمسؤوليات

1. تلتزم الجامعة باعتماد السياسات والإجراءات المتعلقة بحماية البيانات الشخصية، ويكون مدير مكتب إدارة البيانات بالجامعة – أو من يفوضه – مسؤولاً عن الموافقة عليها.
2. يكون مكتب إدارة البيانات بالجامعة مسؤول عن مراقبة تنفيذ السياسات والإجراءات المعتمدة بالجامعة، وتتضمن مهام ومسؤوليات المكتب وضع المعايير المناسبة لتحديد مستويات حساسية البيانات الشخصية.
3. يقوم مكتب إدارة البيانات بتقييم المخاطر والآثار المحتملة لأنشطة معالجة البيانات الشخصية وعرض نتائج التقييم على مدير مكتب إدارة البيانات بالجامعة – أو من يفوضه – لتحديد مستوى قبول المخاطر وإقرارها.
4. تلتزم كافة جهات الجامعة بتطبيق السياسات والإجراءات المتعلقة بحماية البيانات الشخصية المعتمدة وذلك يشمل تحديث العقود واتفاقيات مستوى الخدمة والتشغيل بما يتوافق مع سياسات وإجراءات الخصوصية.
5. تلتزم الأطراف الخارجية التي يسند إليها خدمات معالجة البيانات من الامتثال لهذه السياسة.
6. يحق لمكتب إدارة البيانات بالجامعة وضع قواعد إضافية لمعالجة أنواع محددة من البيانات الشخصية وفقا لطبيعة وحساسية هذه البيانات.

2.4 ضوابط جمع ومعالجة البيانات الشخصية

1. أن يكون الغرض من جمع البيانات الشخصية متوافقًا مع الأنظمة واللوائح والسياسات المعمول بها في المملكة العربية السعودية وذا علاقة مباشرة بنشاط الجامعة.
2. أن يكون محتوى البيانات مقتصرًا على الحد الأدنى من البيانات اللازمة لتحقيق الغرض من جمعها.
3. أن يتم تقييد جمع البيانات على المحتوى المعد سلفًا (الموضح في الضابط السابق - رقم 2) ويكون بطريقة عادلة (مباشرة وواضحة وآمنة وخالية من أساليب الخداع أو التضليل).
4. أن يقتصر استخدام البيانات على الغرض الذي جمعت من أجله.

2.5 آلية جمع ومعالجة البيانات الشخصية

1. إشعار صاحب البيانات - بطريقة ملائمة وقت جمع البيانات - بالغرض والأساس النظامي والاحتياج الفعلي والوسائل والطرق المستخدمة لجمع ومعالجة ومشاركة البيانات الشخصية وكذلك التدابير الأمنية لضمان حماية الخصوصية حسب الأنظمة واللوائح والسياسات المعمول بها في المملكة العربية السعودية.
2. إشعار صاحب البيانات عن المصادر الأخرى التي يتم استخدامها في حال تم جمع بيانات إضافية بطريقة غير مباشرة (من جهات أخرى).
3. تزويد صاحب البيانات بالخيارات المتاحة فيما يتعلق بمعالجة البيانات الشخصية والآلية المستخدمة لممارسة هذه الخيارات، ومنها على سبيل المثال (Preferences, Opt-in and Opt-out).
4. تحديد وتوفير الوسائل التي عن طريقها يمكن لصاحب البيانات الوصول إلى بياناته الشخصية وذلك لمراجعتها وتحديثها.

5. التحقق من هوية الأفراد قبل منحهم الوصول إلى بياناتهم الشخصية وفقا للضوابط المعتمدة من قبل الهيئة الوطنية للأمن السيبراني والجهات ذات الاختصاص.
6. أخذ موافقة صاحب البيانات على معالجة البيانات الشخصية بعد تحديد نوع الموافقة (صريحة أو ضمنية) بناء على طبيعة البيانات وطرق جمعها.
7. إعداد وتوثيق وتطبيق الإجراءات اللازمة لضمان دقة البيانات واكتمالها وحداثتها وارتباطها بالغرض الذي جمعت من أجله.

2.6 مشاركة البيانات الشخصية

1. يحظر مشاركة البيانات الشخصية مع جهات أخرى إلا وفقًا للأغراض المحددة بعد موافقة صاحب البيانات ووفقًا للأنظمة واللوائح والسياسات على أن تزود الجهات الأخرى بسياسات وإجراءات الخصوصية المتبعة وتضمينها في العقود والاتفاقيات.
2. تؤخذ موافقة أصحاب البيانات في حال مشاركة البيانات مع جهات أخرى لاستخدامها في غير الأغراض المحددة، ولهم حق الرفض.
3. أخذ موافقة مدير مكتب إدارة البيانات في حال مشاركة البيانات الشخصية مع جهات أخرى خارج المملكة العربية السعودية.

2.7 ضوابط الاحتفاظ بالبيانات الشخصية

1. يتم تخزين البيانات الشخصية، ومعالجتها داخل الحدود الجغرافية للمملكة، لضمان المحافظة على السيادة الوطنية الرقمية لهذه البيانات. ولا يجوز معالجتها خارج المملكة إلا بعد الحصول على موافقة كتابية من مدير مكتب إدارة البيانات بجامعة الملك عبدالعزيز.
2. عند التخلص من البيانات الشخصية، يتم إتلاف البيانات بطريقة آمنة تمنع فقدانها أو إساءة استخدامها أو الوصول غير المصرح به إليها – وتشمل البيانات التشغيلية، المؤرشفة، والنسخ الاحتياطية – وذلك وفقًا لما يصدر من الهيئة الوطنية للأمن السيبراني.
3. تضمين هذه الضوابط في العقود في حال إسناد هذه المهام إلى جهات معالجة أخرى.

2.8 التدابير الأمنية لحماية البيانات الشخصية

1. منح صلاحيات الوصول إلى البيانات وفقا لمهام العاملين ومسؤولياتهم بناء على مبدأ "الحد الأدنى من الامتيازات" و"الحاجة إلى المعرفة" والمذكورة في سياسة تصنيف البيانات.
2. تطبيق الإجراءات الإدارية والتدابير التقنية التي توثق مراحل معالجة البيانات وتوفر إمكانية تحديد المستخدم المسؤول عن كل مرحلة من هذه المراحل (سجلات الاستخدام).

3. استخدام التدابير الأمنية المناسبة – كالتشفير– لأمن البيانات الشخصية وحمايتها بما يتناسب مع طبيعتها وحساسيتها والوسائط المستخدمة لنقلها وتخزينها وفقًا لما يصدر من الهيئة الوطنية للأمن السيبراني والجهات ذات الاختصاص.
4. مراقبة الامتثال لسياسات وإجراءات الخصوصية بشكل دوري ويتم عرضها على مدير مكتب إدارة البيانات – أو من يفوضه – كما يتم تحديد وتوثيق الإجراءات التصحيحية التي سيتم اتخاذها في حال عدم الامتثال وإشعار المكتب بذلك.

2.9 معالجة انتهاكات الخصوصية

- تلتزم جميع جهات الجامعة بإشعار صاحب البيانات الشخصية فورًا ودون تأخير وبما لا يتجاوز 72 ساعة من وقوع أو اكتشاف أي حادثة تسريب للبيانات الشخصية وفقًا للآليات والإجراءات التي حددها المكتب.
- تلتزم جميع جهات الجامعة إبلاغ مكتب إدارة البيانات بالجامعة فورا ودون تأخير وبما لا يتجاوز 72 ساعة من وقوع أو اكتشاف أي حادثة تسريب للبيانات الشخصية وفقـًا للآليات والإجراءات التي حددها المكتب.
- تلتزم جميع جهات الجامعة بالتعاون في الاستجابة والتحقيق في حوادث انتهاك خصوصية البيانات، والرفع بذلك لمكتب إدارة البيانات بالجامعة لاستكمال الاجراءات النظامية.

2.10 حقوق صاحب البيانات

1. الحق في العلم ويشمل ذلك إشعاره بالأساس النظامي أو الاحتياج الفعلي لجمع بياناته الشخصية، والغرض من ذلك، وألا تعالج بياناته لاحقًا بصورة تتنافى مع الغرض من جمعها والذي من أجله قدم موافقته الضمنية أو الصريحة.
2. الحق في الرجوع عن موافقته على معالجة بياناته الشخصية - في أي وقت – ما لم تكن هناك أغراض مشروعة تتطلب عكس ذلك.
3. الحق في الوصول إلى بياناته الشخصية، وذلك للاطلاع عليها وطلب تصحيحها أو إتمامها أو تحديثها وطلب إتلاف ما انتهت الحاجة إليه منها والحصول على نسخة منها بصيغة واضحة.

3

سياسة مشاركة البيانات

3.1 النطاق

تنطبق أحكام هذه السياسة على جميع البيانات التي تتلقاها، تنتجها أو تتعامل معها جامعة الملك عبدالعزيز، مهما كان مصدرها، شكلها، أو طبيعتها. يشمل ذلك بيانات الطلاب، البيانات الشخصية والمهنية للموظفين، السجلات الأكاديمية والبحثية، المراسلات الإلكترونية والورقية، وكذلك البيانات الناتجة عن الشراكات الخارجية والتفاعلات مع الجهات الأخرى. يغطي أيضًا البيانات المخزنة على أنظمة الجامعة، بما في ذلك السجلات الإدارية، ووسائل التواصل الاجتماعي، والوثائق المكتوبة بخط اليد، والصور، والفيديوهات، والمواد الصوتية، بالإضافة إلى أي أشكال أخرى من البيانات المتعلقة بالأنشطة الأكاديمية والبحثية والإدارية للجامعة.

لا تنطبق أحكام هذه السياسة في حال كانت الجهة الطالبة للبيانات جهة حكومية، وكان الطلب لأغراض أمنية أو لاستيفاء متطلبات قضائية.

3.2 المبادئ الرئيسية لمشاركة البيانات

المبدأ الأول: تعزيز ثقافة المشاركة

تسعى الجامعة لتحقيق التكامل مع الجهات الخارجية والداخلية من خلال تبني "مبدأ المرة الواحدة"، حيث تعمل على مشاركة البيانات الرئيسية التي تمتلكها بفعالية لضمان الحصول على البيانات من مصادرها الصحيحة. هذا يساعد على الحد من ازدواجية البيانات وتعارضها وتعدد مصادرها، مما يرفع من مستوى التعامل مع البيانات كمورد قيّم للبحث، والتعلم، وصنع القرارات. ويعزز هذا التوجه من التطوير والابتكار على مستوى الجامعة والمستوى الوطني من خلال التعاون مع الجهات الأخرى.

المبدأ الثاني: مشروعية الغرض

يتجسد مبدأ "مشروعية الغرض" في التأكيد على أن كل عملية مشاركة بيانات يجب أن تكون مبررة ومحددة الغرض، وتخدم المصالح العامة ومصلحة الجامعة والمجتمع الأكاديمي وتحقق التقدم في مجالات محددة. وأن تكون عملية المشاركة متوافقة مع اللوائح والقوانين المتعلقة بالخصوصية والأمان، وأن تحافظ على حقوق وسلامة جميع الأطراف المعنية وهذا ما يضمن أن مشاركة البيانات تتم بطريقة مسؤولة وتحترم خصوصية وسلامة المعلومات.

المبدأ الثالث: الوصول المصرح به

تمنح الأطراف المشاركة الصلاحية للاطلاع على البيانات والحصول عليها واستخدامها، مع التأكيد على ضرورة تطبيق إجراءات وضوابط دقيقة لضمان الأمان والسرية. يشمل هذا التأكيد على أهلية الأشخاص للتعامل مع البيانات المشتركة بطريقة تضمن الالتزام بأعلى معايير الأمان والخصوصية. هذا يضمن أن الوصول إلى البيانات يتم بطريقة مسؤولة ومحوكمة، بما يحافظ على سلامة وأمن البيانات.

المبدأ الرابع: الشفافية

تعزيزًا للثقة بين الأطراف المعنية وضمان التعامل المسؤول والأخلاقي مع البيانات، يتم التركيز على حماية الخصوصية والسرية من خلال الوضوح والشفافية في جميع مراحل مشاركة البيانات. يشمل ذلك تقديم معلومات دقيقة وشاملة حول آليات جمع البيانات، مصادرها، أهداف استخدامها، وطرق نقلها وتخزينها. كما يتضمن الإفصاح عن أي قيود أو شروط تتعلق بالوصول إلى البيانات ومشاركتها، مما يساهم في ترسيخ بيئة شفافة ومفتوحة لمشاركة البيانات.

المبدأ الخامس: المسؤولية المشتركة

تأكيدًا على الدور الحيوي الذي يلعبه كل طرف مشارك في عملية مشاركة البيانات، يتحمل كل من موفري البيانات ومستخدميها مسؤولية مشتركة في ضمان استخدام البيانات بطريقة أخلاقية وآمنة، ويشمل ذلك ضمان تطبيق الضوابط الأمنية الملائمة، اتخاذ قرارات مسؤولة بشأن مشاركة البيانات وفقًا للسياسات والتشريعات ذات العلاقة، والالتزام بأحكام اتفاقيات مشاركة البيانات. للمساهمة في تعزيز بيئة تعاونية مسؤولة، حيث يكون كل طرف على دراية بأدواره ومسؤولياته في إدارة وحماية البيانات.

المبدأ السادس: أمن البيانات

في إطار "أمن البيانات" يتم الحرص على تطبيق الضوابط الأمنية المناسبة لحماية البيانات ومشاركتها في بيئة آمنة وموثوقة لضمان حماية البيانات في جميع مراحلها - من الجمع والمعالجة إلى المشاركة والتخزين. حيث يتم التركيز على ضرورة تطبيق إجراءات وضوابط أمنية ملائمة لحفظ البيانات من الوصول غير المصرح به أو التلف أو الكشف غير المقصود. يشمل هذا النهج الاستخدام الفعال لأحدث التقنيات وأفضل الممارسات في مجال أمن المعلومات.

المبدأ السابع: الاستخدام الأخلاقي

تعزيزًا للاستخدام الأخلاقي للبيانات، يتم التأكيد على الالتزام بالممارسات الأخلاقية العالية واحترام الخصوصية والسرية وحقوق الملكية الفكرية في جميع جوانب مشاركة واستخدام البيانات. يشمل هذا النهج التزام جميع الأطراف بممارسات تحترم الحقوق الأخلاقية والقانونية لأصحاب البيانات وتضمن الاستخدام الآمن والمسؤول للمعلومات.

3.3 ضوابط مشاركة البيانات

يجب على جميع الأطراف المشاركة في عملية مشاركة البيانات الموافقة على الضوابط اللازمة لإدارة البيانات التي سيتم مشاركتها وحمايتها بشكل مناسب والمعتمدة في سياسة مشاركة البيانات التابعة لمكتب إدارة البيانات الوطنية، وهي كالتالي:

الضابط الأول: الأساس النظامي

(المبادئ ذات العلاقة: المبدأ الأول: تعزيز ثقافة المشاركة، المبدأ الثاني: مشروعية الغرض، المبدأ الخامس: المسؤولية المشتركة، المبدأ السابع: الاستخدام الأخلاقي)

- توضيح الأساس النظامي أو الاحتياج الفعلي لمشاركة البيانات، ومنها على سبيل المثال: تنظيم الجهة، الأمر الملكي/السامي الذي يسمح للجهة بمشاركة البيانات، أو الاتفاقيات الموقعة.
- الالتزام بمستويات تصنيف البيانات والمحافظة على حقوق الملكية الفكرية وخصوصية البيانات الشخصية.

الضابط الثاني: التفويض

(المبادئ ذات العلاقة: المبدأ الثالث: الوصول المصرح به، المبدأ السادس: أمن البيانات)

- تحديد الجهات والأشخاص المخولين بطلب البيانات وتلقيها (يتم التحقق من الامتثال لسياسة تصنيف البيانات – ضوابط الاستخدام والوصول إلى البيانات).

الضابط الثالث: نوع البيانات

(المبادئ ذات العلاقة: المبدأ الأول: تعزيز ثقافة المشاركة، المبدأ الثاني: مشروعية الغرض، المبدأ الرابع: الشفافية)

- التأكد من أن البيانات المطلوبة ضمن البيانات الرئيسية التي تنتجها الجهة لضمان طلب البيانات من مصدرها الصحيح.
- بيان الحد الأنى من البيانات المطلوبة لتحقيق الأغراض المحددة.
- تحديد البيانات المطلوبة وصيغتها والمتطلبات المتعلقة بتعديلها أو تغييرها (مثل صيغة البيانات، دقة البيانات، مستوى التفاصيل، هيكلة البيانات، نوع البيانات خام أو بيانات معالجة).

الضابط الرابع: المعالجة المسبقة للبيانات

(لمبادئ ذات العلاقة: المبدأ السادس: أمن البيانات)

- تحديد ما إذا كان هناك حاجة لمعالجة البيانات قبل مشاركتها، وفي حال الحاجة لذلك يتم الاتفاق على أساليب المعالجة المطلوبة - على سبيل المثال، الحجب وإخفاء الهوية والتجميع (على ألا تتم معالجة البيانات بشكل يغير المحتوى).
- تقييم جودة البيانات المطلوبة وصحتها وسلامتها وتحديد ما إذا كانت تتطلب إجراء تحسين قبل مشاركتها، وفي حال الحاجة لذلك تتم عملية التدقيق على البيانات قبل مشاركتها.

الضابط الخامس: وسائل مشاركة البيانات

(المبادئ ذات العلاقة: المبدأ السادس: أمن البيانات)

- الالتزام بضوابط حماية البيانات التي تصدرها الهيئة الوطنية للأمن السيبراني.
- تحديد وسائل مشاركة البيانات المادية والرقمية.
- التحقق من أمن وموثوقية وسائل المشاركة للتقليل من المخاطر المحتملة، كما يمكن الاستفادة من وسائل المشاركة الآمنة المعتمدة بين الجهات.
- تحديد آلية مشاركة البيانات، وما إذا كان سيتم نقل البيانات مباشرة إلى مقدم الطلب أو سيتم الاستعانة بمقدم خدمة لإتمام عملية المشاركة.
- الاتفاق على آلية إتلاف الوسائط المادية المستخدمة في مشاركة البيانات.

الضابط السادس: استخدام البيانات والحفاظ عليها

(المبادئ ذات العلاقة: المبدأ الثاني: مشروعية الغرض، المبدأ الرابع: الشفافية، المبدأ السادس: أمن البيانات، المبدأ السابع: الاستخدام الأخلاقي)

- تحديد متطلبات حماية البيانات عند مشاركتها، وتطبيق الضوابط المحددة لحماية البيانات بعد مشاركتها.
- فرض قيود مناسبة على الاستخدام أو المعالجة المسموح بها للبيانات (إن وجدت)، مثل (قيود خاصة بالمعالجة أو قيود مكانية أو زمانية، أو حقوق حصرية).
- تحديد حقوق جميع الأطراف المشاركة في عملية المشاركة بإجراء عمليات التدقيق والمراجعة.
- الاتفاق على إجراءات تسوية النزاعات والتحكيم.
- تحديد ما إذا كان هناك طرف ثالث للاستفادة من البيانات بعد مشاركتها والاتفاق على الآلية المنظمة لذلك.

الضابط السابع: مدة مشاركة البيانات وعدد مرات المشاركة وإلغاء المشاركة

(المبادئ ذات العلاقة: المبدأ الثاني: مشروعية الغرض، المبدأ السادس: أمن البيانات)

- تحديد مدة مشاركة البيانات والموعد النهائي للوصول إلى البيانات أو تخزينها.
- تحديد عدد مرات مشاركة البيانات والمتطلبات اللازمة للمراجعة وإجراء التعديلات والإجراءات التي سيتم اتخاذها عند انتهاء الاتفاقية (مثل إخفاء هوية أصحاب البيانات أو إلغاء الوصول إلى البيانات أو إتلافها).
- تحديد الأطراف الذين يحق لهم إنهاء مشاركة البيانات قبل التاريخ المتفق عليه، مع بيان المستند النظامي وفترة الإشعار المسموح بها.

الضابط الثامن: أحكام المسؤولية

(المبادئ ذات العلاقة: المبدأ الخامس: المسؤولية المشتركة)

- الاتفاق على تحديد المسؤوليات في حال عدم الالتزام ببنود الاتفاقية، وغيرها من الالتزامات بين الأطراف المشاركة كإنهاء الاتفاقية والإجراءات التصحيحية.
- تحديد القواعد المتعلقة بأحكام المسؤولية عند مشاركة بيانات خاطئة، وجود مشاكل فنية أثناء عملية نقل البيانات، أو فقدان البيانات بشكل غير مقصود مما قد يتسبب في أضرار أخرى.

3.4 القواعد العامة لمشاركة البيانات

فيما يلي بعض القواعد العامة المعتمدة في سياسة مشاركة البيانات التابعة لمكتب إدارة البيانات الوطنية التي يجب اتباعها عند مشاركة البيانات:

1. يتولى مكتب إدارة البيانات بالجامعة مسؤولية مشاركة البيانات بعد استيفاء جميع مبادئ مشاركة البيانات، بالإضافة إلى تحديد الضوابط المناسبة للمشاركة.
2. تعيين أو تفويض الشخص المناسب –حسب المؤهلات والمنصب المطلوب- للتعامل مع البيانات بطريقة صحيحة، على أن يكون مصرح له طلب البيانات وتلقيها والوصول إليها وتخزينها وإتلافها.
3. إخفاء هوية أصحاب البيانات الشخصية، إلا إذا كان ذلك ضروريًا لغرض المشاركة مع تحديد الضوابط اللازمة للمحافظة على خصوصية أصحاب البيانات وفقـًا لسياسة خصوصية البيانات الشخصية.
4. إرفاق البيانات الوصفية (metadata) عند مشاركة البيانات في الحالات التي تتطلب ذلك.
5. تكون الجهات المشاركة في مشاركة البيانات مسؤولة عن حماية البيانات واستخدامها وفقـًا للأغراض المحددة، ويحق لمكتب إدارة البيانات بجامعة الملك عبدالعزيز مراجعة مدى الالتزام بشكل دوري أو عشوائي بما يتوافق مع الضوابط المحددة في اتفاقية مشاركة البيانات.
6. وجود الدليل الإرشادي لمشاركة البيانات والمتضمن نموذج طلب مشاركة البيانات ونموذج اتفاقية مشاركة البيانات.
7. إعداد الآليات والإجراءات والضوابط المتعلقة بتسوية النزاع وفقـًا لإطار زمني محدد.
8. في حال وجود نزاع بين الأطراف المشاركة في عملية مشاركة البيانات، يحق للجهات التابعة للجامعة إشعار مكتب إدارة البيانات بالجامعة والمطالبة بتسوية النزاع بين الأطراف المشاركة، وفي حال لم يتم حل النزاع، يتم إشعار مكتب إدارة البيانات الوطنية بذلك. ويتولى المكتب تسوية النزاع إذا كانت إحدى الجهات المشاركة غير تابعة للجامعة.
9. في حال وجود جانب من جوانب مشاركة البيانات لا تشملها هذه السياسة، يحق لمكتب إدارة البيانات بالجامعة وضع قواعد إضافية لا تتعارض مع مبادئ مشاركة البيانات مع تقديم مسوغ كاف.
10. يجب على الجهات المشاركة في مشاركة البيانات إيجاد التوازن المناسب بين الحاجة إلى مشاركة البيانات وضمان حماية سرية البيانات والمخاطر المحتملة على الفرد أو المجتمع.
11. يتم الاحتفاظ بسجلات خاصة بطلبات مشاركة البيانات والقرارات المتعلقة بها.
12. لا يمكن للجهات المشاركة أن تشارك البيانات مع طرف آخر إلا بموافقة مكتب إدارة البيانات بالجامعة.

4

سياسة حرية المعلومات

4.1 النطاق

تنطبق أحكام هذه السياسة على جميع طلبات الأفراد أو الجهات للاطلاع أو الحصول على المعلومات العامة (غير المحمية) التي تتلقاها أو تنتجها أو تتعامل معها جامعة الملك عبدالعزيز- سواءً أكانت أنتجت أم استخدمت قبل اعتماد هذه السياسة أم بعدها - مهما كان مصدرها، أو شكلها أو طبيعتها، ويشمل ذلك جميع أشكال البيانات الشخصية المتعلقة بالأفراد.

يُستثنى من نطاق تطبيق هذه السياسة في الأحوال التالية:

1. المعلومات التي قد يؤدي إفشاؤها إلى الإضرار بالأمن الوطني للمملكة العربية السعودية أو سياساتها أو مصالحها أو حقوقها.
2. المعلومات الأمنية بالجامعة.
3. المعلومات والوثائق التي يتم الحصول عليها بمقتضى اتفاق مع دولة أخرى وتصنف على أنها مقيدة.
4. التحريات والتحقيقات وأعمال الضبط وعمليات التفتيش والمراقبة المتعلقة بجريمة أو مخالفة أو تهديد داخل الجامعة.
5. المعلومات التي تتضمن توصيات أو اقتراحات أو استشارات من أجل إصدار تشريع أو قرار لم يصدر بعد.
6. المعلومات ذات الطبيعة التجارية أو الصناعية أو المالية أو الاقتصادية التي يؤدي الإفصاح عنها إلى تحقيق ربح أو تلافي خسارة بطريقة غير مشروعة.
7. الأبحاث العلمية أو التقنية أو الحقوق المشتملة على حق من حقوق الملكية الفكرية التي يؤدي الكشف عنها إلى المساس بحق معنوي.
8. المعلومات المتعلقة بالمنافسات والعطاءات والمزايدات التي يؤدي الإفصاح عنها إلى الإخلال بعدالة المنافسة.
9. المعلومات التي تكون سرية أو شخصية بموجب نظام آخر، أو تتطلب إجراءات نظامية معينة للوصول إليها أو الحصول عليها.

4.2 المبادئ الرئيسية لحرية المعلومات

المبدأ الأول: المسؤولية

للفرد الحق في معرفة المعلومات المتعلقة بأنشطة الجامعة تعزيزًا لمنظومة النزاهة والشفافية والمساءلة داخل الجامعة.

المبدأ الثاني: الضرورة والتناسب

أي قيود على طلب الاطلاع أو الحصول على المعلومات المقيدة التي تتلقاها أو تنتجها أو تتعامل معها الجامعة يجب أن تكون مسوغة بطريقة واضحة وصريحة.

المبدأ الثالث: الأصل في المعلومات العامة الإفصاح

لكل فرد الحق في الاطلاع على المعلومات العامة – غير المقيدة – وليس بالضرورة أن يتمتع مقدم الطلب بحيثية معينة أو باهتمام معين بهذه المعلومات ليتمكن من الحصول عليها، كما لا يتعرض لأي مساءلة قانونية متعلقة بهذا الحق.

المبدأ الرابع: المساواة

يتم التعامل مع جميع طلبات الاطلاع أو الحصول على المعلومات العامة على أساس المساواة وعدم التمييز بين الأفراد.

4.3 حقوق الأفراد بما يتعلق بالاطلاع على المعلومات العامة أو الحصول عليها

1. حق الاطلاع والحصول على المعلومات العامة (الغير مقيدة) لدى الجامعة.
2. الحق في معرفة سبب رفض الاطلاع أو الحصول على المعلومات المطلوبة.
3. الحق في التظلم على قرار رفض طلب الاطلاع والحصول على المعلومات المطلوبة.

4.4 التزامات مكتب إدارة البيانات بجامعة الملك عبدالعزيز

1. إعداد وتطبيق السياسات والإجراءات المتعلقة بممارسة حق الوصول إلى المعلومات العامة أو الحصول عليها.
2. تطوير وتوثيق ومراقبة تنفيذ السياسات والإجراءات المعتمدة والمتعلقة بحق الوصول إلى المعلومات على أن تتضمن مهام ومسؤوليات المكتب وضع المعايير المناسبة لتحديد مستويات تصنيف البيانات في حال عدم وجودها – وفقا لسياسة تصنيف البيانات – واستخدامها كمرجع رئيسي عند معالجة طلبات الاطلاع على المعلومات العامة أو الحصول عليها.
3. توفير الوسائل الممكنة (نماذج طلب المعلومات العامة) – سواء أكانت نماذج ورقية أو إلكترونية – والتي من خلالها يمكن للفرد طلب الاطلاع على المعلومات العامة أو الحصول عليها.
4. التحقق من هوية الأفراد قبل منحهم حق الاطلاع على المعلومات العامة أو الحصول عليها وفقا للضوابط المعتمدة من قبل الهيئة الوطنية للأمن السيبراني والجهات ذات العلاقة.
5. توثيق جميع سجلات طلبات الوصول إلى المعلومات أو الحصول عليها والقرارات المتخذة حيال الطلبات، على أن يتم مراجعة هذه السجلات لمعالجة حالات سوء الاستخدام أو عدم الاستجابة، وفقا للأنظمة والتشريعات ذات العلاقة بذلك.
6. إشعار الفرد - بطريقة ملائمة – في حال تم رفض الطلب كليا أو جزئيا، مع إيضاح أسباب الرفض وله الحق في التظلم وكيفية ممارسة هذا الحق خلال مدة لا تتجاوز (10) أيام من تاريخ الإشعار.

4.5 المتطلبات الرئيسية للحصول على المعلومات العامة أو الاطلاع عليها

1. يجب أن يكون الطلب خطيًا أو إلكترونيًا.
2. يجب تعبئة "نموذج طلب معلومات عامة" المعتمد من قبل مكتب إدارة البيانات بالجامعة.
3. يجب أن يكون الطلب لأغراض الوصول إلى المعلومات العامة أو الحصول عليها.
4. يجب أن يتضمن نموذج الطلب تفاصيل التواصل مع الفرد (الاسم، العنوان الوطني أو البريد الإلكتروني أو موقع الجهة... الخ).
5. يجب إرسال نموذج الطلب مباشرة إلى مكتب إدارة البيانات بالجامعة.

4.6 أحكام عامة

1. يضمن مكتب إدارة البيانات بالجامعة تكامل هذه السياسة مع بقية الوثائق التنظيمية والتشريعية للجامعة.
2. تلتزم الجامعة بعمل توازن بين حق الاطلاع على المعلومات وضرورة حماية البيانات.
3. يجب على جهات الجامعة الامتثال لهذه السياسة ويتولى مكتب إدارة البيانات بالجامعة مراقبة وتدقيق الامتثال لذلك دوريًا.
4. يتولى مكتب إدارة البيانات بالجامعة مسؤولية تلقي التظلمات وإعداد آليات التعامل معها.
5. يجب امتثال الأطراف الخارجية المتعاقدة مع الجامعة لهذه السياسة.
6. يحق للجامعة ممثلة بمكتب إدارة البيانات إضافة قواعد أخرى حسب ما تقتضيه المعلومات المطلوبة.

4.7 حرية المعلومات والبيانات المفتوحة

تأمل الجامعة من مقدمي طلبات الحصول على معلومات عامة، الاطلاع على منصة البيانات المفتوحة قبل تقديم أي طلبات توفيرًا للوقت والجهد والنفقات.

5

سياسة البيانات المفتوحة

5.1 النطاق

تنطبق أحكام هذه السياسة على جميع البيانات والمعلومات العامة (غير المقيدة) التي تتلقاها أو تنتجها أو تتعامل معها جامعة الملك عبدالعزيز- سواءً أكانت أنتجت أم استخدمت قبل اعتماد هذه السياسة أم بعدها - مهما كان مصدرها، أو شكلها أو طبيعتها.

5.2 المبادئ الرئيسية للبيانات المفتوحة

المبدأ الأول: الأصل في البيانات الاتاحة

الأصل في البيانات أن تكون متاحة "عامة" ما لم تقتض طبيعتها أو حساسيتها مستويات أعلى من التصنيف والحماية.

المبدأ الثاني: الصيغة المفتوحة وإمكانيه القراءة

يتم إتاحة البيانات وتوفيرها بصيغة مقروءة تسمح بمعالجتها بشكل آلي بحيث يتم حفظها بصيغ الملفات شائعة الاستخدام مثل (CSV، او XLS، او JSON، او XML).

المبدأ الثالث: حداثة البيانات المفتوحة

تنشر أحدث إصدار من مجموعات البيانات (Data Sets) المفتوحة بصفة منتظمة وتعطى الأولوية للبيانات التي تقل فائدتها بمرور الوقت ويتم إتاحتها للجميع حال توافرها. كما يتم نشر البيانات المجمعة في أسرع وقت ممكن بمجرد جمعها، كلما أمكن ذلك.

المبدأ الرابع: الشمولية

يجب أن تكون مجموعات البيانات المفتوحة شاملة وتتضمن أكبر قدر ممكن من التفاصيل، وأن تعكس البيانات المسجلة بما لا يتعارض مع سياسة حماية البيانات الشخصية؛ كما يجب إدراج البيانات الوصفية التي توضح وتشرح البيانات.

المبدأ الخامس: عدم التمييز

تتاح مجموعات البيانات للجميع دون تمييز ودون حاجة للتسجيل ليكون بإمكان أي شخص الوصول إلى البيانات المفتوحة المنشورة في أي وقت دون الحاجة إلى التحقق من الهوية أو تقديم مسوغ للوصول إليها.

المبدأ السادس: الرسوم المالية

تتاح البيانات المفتوحة للجميع مجانًا دون أخذ رسوم أو أجر استخدام من قبل الراغبين في الحصول عليها.

المبدأ السابع: ترخيص البيانات المفتوحة في المملكة

تخضع البيانات المفتوحة في جامعة الملك عبدالعزيز لرخصة البيانات المفتوحة الخاصة بها، التي تحدد الأسس النظامية لاستخدامها، والشروط والالتزامات والقيود المفروضة على المستخدم، كما أن الوصول إلى البيانات المفتوحة يعد قبولاً للشروط المحددة في رخصة البيانات المفتوحة.

المبدأ الثامن: تطوير نموذج الحوكمة وإشراك الجميع

تمكن البيانات المفتوحة عملية الاطلاع والمشاركة للجميع، وتعزز الشفافية وتدعم عملية صنع القرار وتقديم الخدمات.

المبدأ التاسع: التنمية الشاملة والابتكار

تلعب الجامعة دورًا فعالاً في تعزيز استخدام البيانات وتوفير الموارد والخبرات اللازمة الداعمة للتنمية والابتكار والعمل بتكامل بين جهاتها الداخلية على تمكين الأفراد والمؤسسات والجميع بوجه عام في إطلاق القدرات البحثية والابتكار من خلال الاستفادة من البيانات المفتوحة.

5.3 القواعد العامة للبيانات المفتوحة

تمتثل جامعة الملك عبدالعزيز ممثلةً في مكتب إدارة البيانات بالقواعد العامة لسياسة البيانات المفتوحة خلال مراحل دورة حياة البيانات المفتوحة، وتشمل:

- وضع خطط النشر.
- تحديد البيانات المفتوحة.
- نشر البيانات المفتوحة.
- تحديث البيانات المفتوحة.
- متابعة أداء البيانات المفتوحة.

5.4 الامتثال

1. تلتزم الجامعة ممثلة في مكتب إدارة البيانات بسياسة البيانات المفتوحة وتقدم تقرير سنوي إلى مكتب إدارة البيانات الوطني يشمل، على سبيل المثال لا الحصر، ما يلي:
   - التقدم ومستوى الإنجاز الذي حققته الجامعة في خطتها المحددة.
   - الأهداف ومؤشرات الأداء الرئيسية المحددة في خطة البيانات المفتوحة.
   - عدد مجموعات البيانات المفتوحة المحددة.
   - عدد مجموعات البيانات المفتوحة المنشورة.
2. تقييم الامتثال لسياسة البيانات المفتوحة من خلال الحرص الدائم والمستمر على تطبيق هذه السياسة، ووضع تقييم دوري ومراجعة للبيانات المنشورة أو القابلة للنشر.
3. عند وجود نقاط عدم امتثال، يقوم مكتب إدارة البيانات بالجامعة العمل على تصحيحها من خلال إجراءات تصحيحية، تشمل التوعية، والتعاون، والتدخل المباشر.

6

سياسة حماية البيانات الشخصية للأطفال ومن في حكمهم

6.1 النطاق

تنطبق أحكام هذه السياسة على جميع البيانات الشخصية التي تتلقاها أو تنتجها أو تتعامل معها جامعة الملك عبدالعزيز- سواءً أكانت أنتجت أم استخدمت قبل اعتماد هذه السياسة أم بعدها - مهما كان مصدرها، أو شكلها أو طبيعتها، ويشمل ذلك جميع أشكال البيانات الشخصية المتعلقة بالأفراد.

يُستثنى من نطاق تطبيق هذه السياسة في الأحوال التالية:

- إذا كان جمع البيانات الشخصية أو معالجتها مطلوبًا لتحقيق متطلبات نظامية وفقًا للأنظمة واللوائح والسياسات المعمول بها في المملكة أو لاستيفاء متطلبات قضائية أو لتنفيذ التزام بموجب اتفاق تكون المملكة طرفًا فيه.
- إذا كان جمع البيانات الشخصية أو معالجتها ضروريًا لحماية الصحة أو السلامة العامة أو حماية المصالح الحيوية للأفراد.

6.2 حقوق الطفل ومن في حكمه فيما يتعلق بمعالجة بياناته الشخصية

1. يُمنح الطفل ومن في حكمه جميع الحقوق المنصوص عليها في سياسة البيانات الشخصية الصادرة من مكتب إدارة البيانات بالجامعة ويتم ممارسة هذه الحقوق من قبل ولي الطفل.
2. أحقية الطفل ومن في حكمه طلب إتلاف بياناته الشخصية بعد بلوغه السن النظامية أو انتهاء الولاية عليه.

6.3 المبادئ الرئيسية لحماية البيانات الشخصية للأطفال ومن في حكمهم

يتم اتباع المبادئ الرئيسية المنصوص عليها في سياسة حماية البيانات الشخصية، بالإضافة لذلك، وبدون الإخلال بتلك المبادئ تلتزم جامعة الملك عبدالعزيز بالقواعد الإضافية التالية التي تضمن المحافظة على خصوصية الأطفال ومن في حكمهم وحماية حقوقهم والمتمثلة في:

1. إشعار ولي الطفل عن المصادر الأخرى التي يتم استخدامها في حال تم جمع بيانات إضافية وموافاته بالخيارات المتاحة بشأن معالجة البيانات الشخصية للأطفال ومن في حكمهم والآليات المستخدمة.
2. أن يكون الغرض من جمع البيانات الشخصية للأطفال ومن في حكمهم متوافقًا مع الأنظمة ذات الصلة وذو علاقة مباشرة بنشاط الجامعة.
3. أن يكون محتوى البيانات مقتصرًا على الحد الأدنى من البيانات اللازمة لتحقيق الغرض من جمعها.
4. أن يتم تقييد جمع البيانات الشخصية للأطفال ومن في حكمهم على المحتوى المعد سلفًا (الموضح في القاعدة 3) ويكون بطريقة عادلة (مباشرة وواضحة وآمنة وخالية من أساليب الخداع أو التضليل).
5. أن يقتصر استخدام البيانات على الغرض التي جمعت من أجله والذي تمت الموافقة عليه من قبل ولي الطفل.

6.4 أدوار ومسؤوليات جامعة الملك عبدالعزيز

1. تلتزم الجامعة بإشعار ولي الطفل وأخذ الموافقة منه في حال مشاركة البيانات مع جهات أخرى لاستخدامها في غير الأغراض المحددة.
2. تلتزم الجامعة بإشعار ولي الطفل في حال الرغبة في التواصل مع الطفل أو من في حكمه بطريقة مباشرة لأي غرض كان وإتاحة الفرصة له لرفض هذا التواصل مع إيضاح أسباب ذلك.
3. تلتزم الجامعة بعدم جمع بيانات شخصية من الطفل أو من في حكمه تتعلق بأحد أفراد أسرته في أي حال من الأحوال، ماعدا البيانات الشخصية لولي الطفل.
4. تلتزم الجامعة بالتحقق من هوية ولي الطفل قبل منحه الوصول إلى بيانات الطفل الشخصية ومن في حكمه وفقًا للضوابط المعتمدة من قبل الهيئة الوطنية للأمن السيبراني والجهات ذات الاختصاص.
5. تلتزم الجامعة بتحديد وتوفير الوسائل التي من خلالها يمكن لولي الطفل الوصول إلى البيانات الشخصية للطفل ومن في حكمه وذلك لمراجعتها وتحديثها.
6. تلتزم الجامعة باستخدام الضوابط والتدابير والضمانات القانونية الكافية لحماية البيانات الشخصية للأطفال ومن في حكمهم.
7. تلتزم الجامعة بعدم اتخاذ إجراءات آلية بناءً على معالجة البيانات الشخصية للأطفال ومن في حكمهم واستخدامها لأغراض متعددة لها تأثير كبير عليهم، ومنها على سبيل المثال (التسويق المباشر).
8. تلتزم الجامعة بتطبيق التدابير المناسبة التي تمنع إتاحة البيانات الشخصية للأطفال ومن في حكمهم للجمهور بطريقة يمكن من خلالها التعرف عليهم وعلى أسرهم بشكل مباشر.
9. تلتزم الجامعة بعدم مشاركة البيانات الشخصية للأطفال ومن في حكمهم مع جهات أخرى إلا وفقًا للأغراض المحددة بعد موافقة ولي الطفل ووفقًا للأنظمة واللوائح والسياسات ذات الصلة على أن يتم تزويد الجهات الأخرى بالسياسات والإجراءات المتعلقة بحماية البيانات الشخصية للأطفال ومن في حكمهم وتضمينها في العقود والاتفاقيات.
10. تلتزم الجامعة بأخذ موافقة ولي الطفل على معالجة البيانات الشخصية للأطفال ومن في حكمهم بعد تحديد نوع الموافقة (صريحة أو ضمنية) بناءً على طبيعة البيانات وطرق جمعها.

6.5 قواعد يُستثنى منها موافقة ولي الطفل

1. لا يشترط الحصول على موافقة ولي الطفل إذا كانت الخدمة المقدمة للطفل أو من في حكمه هي خدمة وقائية أو استشارية وفقًا لمهام واختصاصات الجامعة.
2. لا يشترط الحصول على موافقة ولي الطفل في حال الإفصاح عن بياناته الشخصية لطرف ثالث من أجل تنفيذ التزام مشروع على الجامعة أو لتنفيذ اتفاقية تكون المملكة العربية السعودية طرفًا فيه أو كانت الجهة التي سيتم الإفصاح لها جهة قضائية أو أمنية.
3. لا يشترط الحصول على موافقة ولي الطفل عندما يكون الغرض الوحيد من جمع بيانات الاتصال بالطفل أو من في حكمه هو الرد مباشرة على طلب محدد من الطفل ومن في حكمه.
4. لا يشترط الحصول على موافقة ولي الطفل عندما يكون الغرض من جمع بيانات الاتصال للولي والطفل ومن في حكمه هو الاستجابة مباشرة – مرة أو أكثر - لطلب الطفل ومن في حكمه المحدد، ولا يتم استخدام هذه البيانات لأي غرض آخر، ولا يتم الإفصاح عنها، أو دمجها مع أي بيانات أخرى، ويتم تزويد الولي بإشعار بذلك.
5. لا يشترط الحصول على موافقة ولي الطفل عندما يكون الغرض من جمع اسم الطفل ومن في حكمه واسم ولي الطفل وبيانات الاتصال هو حماية سلامة الطفل ومن في حكمه، ولا يتم استخدام هذه البيانات أو الكشف عنها لأي غرض لا علاقة له بسلامة الطفل ومن في حكمه، ويتم تزويد الولي بإشعار بذلك.

6.6 الأحكام الخاصة المتعلقة بولي الطفل

1. يحق للجامعة أن تحصل على البيانات الشخصية للولي من الطفل ومن في حكمه مباشرة، مع الالتزام بالحصول على الحد الأدنى من البيانات اللازمة – الاسم وطريقة التواصل مع ولي الطفل – فقط من أجل إشعار ولي الطفل والحصول على موافقته.
2. تلتزم الجامعة باستخدام الوسائل المناسبة للتحقق من هوية ولي الطفل قبل أخذ موافقته ومنحه الوصول إلى بيانات الطفل الشخصية ومن في حكمه وفقًا للضوابط المعتمدة من قبل الهيئة الوطنية للأمن السيبراني والجهات ذات الاختصاص.
3. في حال تم طلب موافقة ولي الطفل ولم يقدم موافقته خلال (10) أيام من تاريخ التواصل معه، يتم إتلاف بيانات الطفل الشخصية ومن في حكمه وبيانات الولي التي جمعت.
4. تلتزم الجامعة بعدم استخدام البيانات الشخصية لولي الطفل لغير الغرض الذي جمعت من أجله في حدود الموافقة على جمع ومعالجة البيانات الشخصية للطفل ومن في حكمه.
5. تلتزم الجامعة بإشعار ولي الطفل بالطلبات المقدمة من الطفل ومن في حكمه فيما يتعلق بالبيانات الشخصية له وأخذ موافقته عليها.

6.7 ضوابط الاحتفاظ بالبيانات الشخصية للأطفال ومن في حكمهم

1. يتم تخزين البيانات الشخصية للأطفال ومن في حكمهم، ومعالجتها داخل الحدود الجغرافية للمملكة، لضمان المحافظة على السيادة الوطنية الرقمية لهذه البيانات. ولا يجوز معالجتها خارج المملكة إلا بعد الحصول على موافقة كتابية من مدير مكتب إدارة البيانات بجامعة الملك عبدالعزيز و ولي الطفل.
2. عند التخلص من البيانات الشخصية للأطفال ومن في حكمهم، يتم إتلاف البيانات بطريقة آمنة تمنع فقدانها أو إساءة استخدامها أو الوصول غير المصرح به إليها – وتشمل البيانات التشغيلية، المؤرشفة، والنسخ الاحتياطية – وذلك وفقـًا لما يصدر من الهيئة الوطنية للأمن السيبراني.
3. تضمين هذه الضوابط في العقود في حال إسناد هذه المهام إلى جهات معالجة أخرى.

7

القواعد العامة لنقل البيانات الشخصية خارج الحدود الجغرافية للمملكة العربية السعودية

7.1 النطاق

تنطبق أحكام هذه السياسة على جميع البيانات الشخصية والمشمولة بنطاق تطبيق سياسة حماية البيانات الشخصية عند نقل البيانات الشخصية إلى جهات خارج الحدود الجغرافية للمملكة العربية السعودية بغرض معالجتها.

7.2 حقوق أصحاب البيانات

يُمنح صاحب البيانات ومن في حكمه جميع الحقوق المنصوص عليها في سياسة البيانات الشخصية الصادرة من مكتب إدارة البيانات بالجامعة، مع التأكيد على الحقوق التالية:

- **الحق في العلم:**

  يشمل ذلك إشعاره بالأساس النظامي أو الاحتياج الفعلي لنقل بياناته الشخصية خارج الحدود الجغرافية للمملكة العربية السعودية ومكان تخزينها أو استضافتها، والجهات التي سيتم الإفصاح لها عن بياناته الشخصية عند نقلها، والغرض من هذا النقل، وأخذ موافقته على ذلك.

- **الحق في الرجوع عن موافقته:**

  يحق لصاحب البيانات الرجوع عن موافقته على معالجة بياناته الشخصية خارج الحدود –في أي وقت– مالم يكن الغرض من نقل البيانات تحقيقـًا للمصلحة العامة، أو حمايةً للمصالح الحيوية للأفراد، أو تنفيذًا لمتطلبات نظامية.

- **الحق في الوصول إلى بياناته الشخصية:**

  يحق لصاحب البيانات الوصول لبياناته الشخصية لدى الجامعة أو جهة المعالجة الخارجية، وذلك للاطلاع عليها، وطلب تصحيحها، أو إتمامها، أو تحديثها، وطلب إتلاف ما انتهت الحاجة إليه منها، والحصول على نسخة منها.

الأصل في معالجة البيانات أن تكون داخل الحدود الجغرافية للمملكة العربية السعودية ولا يجوز نقلها او معالجتها خارج المملكة إلا بعد التحقق من الحالات الموضحة أدناه حسب التسلسل التالي:

1. أن تكون جهة معالجة البيانات الشخصية خارج المملكة في دولة مشمولة بالقائمة المعتمدة لدى مكتب إدارة البيانات الوطنية.
2. إذا كانت الجهة الخارجية التي نُقلت إليها البيانات الشخصية غير مشمولة بقائمة الاعتماد، يتطلب منها مستوى كاف من الحماية لا يقل عن المستوى المعتمد في سياسة حماية البيانات الشخصية.
3. إذا لم يكن هناك مستوى كاف من الحماية، فتقوم الجامعة ممثلة في مكتب إدارة البيانات بوضع ضمانات مناسبة لحماية حقوق أصحاب البيانات، بما يتناسب مع متطلبات مكتب إدارة البيانات الوطنية وهيئة الأمن السيبراني.
4. إذا لم يتم توفير الضمانات الأمنية الكافية لحماية البيانات الشخصية فيمكن لجهة المعالجة الحصول على الاستثناء اللازم وفق التنظيمات ذات العلاقة الصادرة من مكتب إدارة البيانات الوطنية وهيئة الأمن السيبراني.

أولاً: تقييم مستوى الحماية

يقوم مكتب إدارة البيانات بالجامعة بإجراء تقييم الآثار والمخاطر المحتملة – كل حالة على حدة – لتحديد ما إذا كان سيتم توفير مستوى كاف من الحماية لحقوق أصحاب البيانات وعرض نتائج التقييم على مدير مكتب إدارة البيانات لتحديد مستوى قبول المخاطر وإقرارها. وللقيام بذلك يجب أن يقدم ما يثبت الالتزام بمعايير التقييم التالية:

أ- معايير التقييم العامة

1. نوع البيانات وقيمتها وحجمها المراد نقلها لتحديد مستوي الحماية المطلوبة.
2. الغرض من معالجة البيانات، وفئة أصحاب البيانات، ونطاق المعالجة، والجهات التي سيتم مشاركتها.
3. الفترة التي يتم خلالها معالجة البيانات.
4. مستوى الحماية في الدولة التي سيتم نقل البيانات لها.
5. مستوى الحماية في المراحل التي يتم بها نقل البيانات الشخصية – والتي قد تمر بأكثر من دولة أحيانا – وتقييم مستوى الحماية في الدولة التي تعد هي الوجهة النهائية.
6. الإجراءات الإدارية والتدابير التقنية والضوابط المادية المعتمدة في سياسات الجهة الخارجية لأمن المعلومات، كالتشفير والضوابط الأمنية والمعايير الدولية.
7. إذا لم يكن هناك مستوى كاف من الحماية، تقوم الجهة بوضع ضمانات مناسبة لحماية حقوق أصحاب البيانات، بما يتناسب مع متطلبات مكتب إدارة البيانات الوطنية وهيئة الأمن السيبراني.
8. إذا لم تتمكن الجهة من توفير الضمانات الأمنية الكافية لحماية البيانات الشخصية، يمكن الحصول على الاستثناء اللازم وفق التنظيمات ذات العلاقة الصادرة من مكتب إدارة البيانات الوطنية وهيئة الأمن السيبراني.

ب- معايير التقييم القانونية

1. وجود أنظمة وتشريعات في الدولة التي يُراد نقل البيانات إليها التي تحمي حقوق أصحاب البيانات.
2. وجود اتفاقيات دولية أو تبني مبادئ ومعايير دولية لحماية البيانات الشخصية في الدولة التي يُراد نقل البيانات إليها.
3. اعتماد قواعد سلوكية أو ممارسات عامة خاصة لحماية البيانات الشخصية في الدولة التي يُراد نقل البيانات إليها.

ثانيًا: الضمانات المناسبة

إذا كانت الجهة المنقول لها البيانات في دولة ليست من ضمن قائمة الاعتماد ولم تخضع لتقييم مستوى الحماية أو كان مستوى الحماية غير كاف، فيجب عليها توفير الضمانات المناسبة لحماية البيانات الشخصية، ومنها:

1. تضمين بنود نموذجية أو قياسية – في العقود والاتفاقيات يتم الموافقة عليها من قبل مكتب إدارة البيانات بالجامعة وذلك لضمان المحافظة على خصوصية البيانات وأصحابها وحماية حقوقهم.
2. إعداد قواعد مشتركة ملزمة قانونيًا تنطبق على عمليات نقل البيانات الشخصية خارج الحدود بما في ذلك معالجة انتهاكات الخصوصية والإشعار عنها - على أن تتم الموافقة عليها من قبل مكتب إدارة البيانات بالجامعة - يتم تضمين هذه القواعد المشتركة كملحقًا لاتفاقيات مستوى الخدمة أو العقود المبرمة بين الجهتين مع أخذ موافقة الأطراف عند وجود أي التزام قانوني تخضع له أي من هذه الأطراف.
3. استخدام قواعد السلوك المعتمدة من قبل مكتب إدارة البيانات الوطنية وهيئة الأمن السيبراني بصفتها أداة فعالة تحدد الالتزامات وذلك لضمان المحافظة على خصوصية أصحاب البيانات وحماية حقوقهم.
4. الاستعانة بأطراف خارجية مستقلة تتولى إصدار شهادات اعتماد تؤكد وجود الضمانات المناسبة للمحافظة على خصوصية أصحاب البيانات وحماية حقوقهم.
5. توقيع اتفاقية ملزمة قانونيا لنقل البيانات الشخصية على أن تتضمن هذه الاتفاقية على بنودًا تعاقدية ملزمة تضمن المحافظة على خصوصية أصحاب البيانات وتحمي حقوقهم.

ثالثًا: الاستثناءات لحالات محددة

يمكن للجهات نقل البيانات الشخصية خارج الحدود الجغرافية للمملكة العربية السعودية دون الالتزام بالشروط والأحكام الموضحة في البند (أولاً) والبند (ثانيًا) أعلاه في حالات محددة، ومنها أن يكون نقل البيانات خارج الحدود الجغرافية للمملكة وفقـًا لما يلي:

1. استنادًا على موافقة أصحاب البيانات.
2. تنفيذًا لالتزام تعاقدي للجامعة.
3. تنفيذًا لمتطلبات قضائية.
4. تنفيذًا لأحكام اتفاقية دولية تكون المملكة طرفـًا فيها.
5. المحافظة على المصلحة العامة بما في ذلك حماية الصحة أو السلامة العامة.
6. حماية المصالح الحيوية لأصحاب البيانات.

7.4 أحكام عامة

1. يتم أخذ موافقة كتابية من مدير مكتب إدارة البيانات بالجامعة لاعتماد عملية نقل البيانات الشخصية خارج الحدود الجغرافية للمملكة.
2. يحق لمكتب إدارة البيانات بالجامعة وضع قواعد إضافية لنقل أنواع محددة من البيانات الشخصية وفقـًا لطبيعة وحساسية هذه البيانات.
3. يتم مراجعة معايير التقييم – العامة والقانونية – المتعلقة بحماية البيانات الشخصية عند نقلها خارج الحدود الجغرافية للمملكة العربية السعودية واتخاذ الاجراءات المنظمة لها.
4. يتم وضع قائمة محددة للعوامل الرئيسية التي تحدد مستوى الحماية المناسب، ومنها على سبيل المثال، الأنظمة والتشريعات، حماية الحقوق والحريات، الأمن الوطني، قواعد حماية البيانات الشخصية.
5. التحقق بشكل دوري من امتثال جهات المعالجة لهذه القواعد.

مكتب إدارة البيانات

Data Management Office

DMO@kau.edu.sa