EVERYONE`S SMART UNIVERSITY

EVERYONE`S SMART UNIVERSITY

سياسة الخصوصية

الهدف يتم تطبيق سياسة الخصوصية على جميع أنظمة الجامعة لغرض التأكد من خصوصية المعلومات الحساسة الخاصة بالطلبة ويلتزم جميع الموظفين باتباع هذه السياسات :

١ - تعرف المعلومات الشخصية بأنها "أي معلومة عن شخصٍ ما، ويتضمن ذلك المعلومات التي يمكن استخدامها لتمييز الأفراد كالاسم، أو المستخدمة لمتابعتهم والوصول إليهم كالعنوان البريدي وأرقام الهواتف، أو أي معلومات يمكن ربطها بالأفراد كالسجلات الطبية.

٢ - إن إدارة الجامعة مسؤولة عن ضمان تنفيذ السياسة وما يتعلق بها من وثائق، ومراقبة علمية التطبيق، واتخاذ الإجراءات المناسبة في حال عدم الالتزام بها.

٣ - تقوم إدارة أمن المعلومات بمراجعة هذه السياسة ومدى الالتزام بها وإصدار تقرير بذلك، وذلك لمرة واحدة خلال العام على أقل تقدير.

٤ - يجب نشر هذه السياسة فور اعتمادها من إدارة الجامعة بحيث يمكن لجميع المستخدمين في جامعة الجميع الذكية الاطلاع عليها. وعلى إدارة أمن المعلومات وإدارة تقنية المعلومات الحرص على وصول التنبيه اللازم بصدورها لجميع المستخدمين وبجميع الطرق الممكنة. كما ويجب أيضاً تنبيه المستخدمين في حال حدوث تعديل على السياسة أو نشر أي سياسة أو وثيقة متممة.

٥ - على جميع المستخدمين الالتزام التام ببنود هذه الاتفاقية وجميع الوثائق المتممة لها.

٦ - إن وصول تنبيه بتوافر هذه السياسة للمستخدمين أو المتعاملين مع الجامعة من داخل الجامعة أو خارجها يعد إشعاراً ضمنيا بقراءة السياسة بجميع بنودها والموافقة ضمنياً على العمل بجميع بنودها.

أنواع المعلومات الشخصية

- معلومات تمييز الأفراد: وهي المعلومات التي يمكن من خلالها تمييز فرد بعينه، مثل الاسم الكامل، أو أحد أجزائه بأي سياق يمكن أن يدل على شخص بعينه مثل رقم الهوية الوطنية ورقم جواز السفر ورقم الحساب البنكي.
- معلومات متابعة الأفراد: وهي المعلومات التي يمكن من خلالها الوصول لشخص معين بشكل شخصي، مثل: العنوان البريدي وعناوين البريد الإلكتروني الشخصية والأرقام الهاتفية الشخصية بكافة أنواعها والأسماء التعريفية على شبكات التواصل الاجتماعي.

٧ - تتعهد جامعة الجميع الذكية ممثلةً بإدارة تقنية المعلومات ببذل أقصى الجهود وتوفير جميع التقنيات والموارد اللازمة لحماية المعلومات الشخصية من الحذف أو التلف أو الضياع أو التسرب أو التعديل، أو أي استخدام آخر غير مصرح به.

٨ - تقود إدارة أمن المعلومات بحفظ سجل عن المعلومات الشخصية، يسمى "دليل المعلومات الشخصية"، ويعرف أحد أعضاء فريق أمن المعلومات كمسؤول لحماية المعلومات الشخصية.

٩ - يكون مسؤول حماية المعلومات الشخصية مسؤولاً عن إدارة الدليل.

١٠ - يكون مسؤول حماية المعلومات الشخصية مسؤولاً عن صحة المعلومات الواردة في "دليل المعلومات الشخصية" بشكل مستمر، وعن جميع عمليات التدقيق لضمان اتباع جميع الأنظمة والمستخدمين للإجراءات والإرشادات الواردة في الدليل.

١١ - على إدارة تقنية المعلومات في الجامعة توفير التقنيات والإجراءات الكفيلة بحصر أماكن تواجد جميع أشكال المعلومات الشخصية على جميع الأنظمة المعلوماتية التي تعود ملكيتها للجامعة.

١٢ - بعد حصر المعلومات الشخصية، يجب أن يتم توثيقها ضمن "دليل المعلومات الشخصية"، على أن يتضمن ذلك:

نوع المعلومة: معلومات تميز الأفراد - معلومات متابعة الأفراد وحساسية المعلومات بحيث يتم تصنيف جميع المعلومات الشخصية في الجامعة بحسب حساسيتها لأحد الأصناف الثلاثة: معلومات منخفضة الحساسية - معلومات متوسطة الحساسية معلومات عالية الحساسية

١٣ - يجب أن يتضمن دليل المعلومات الشخصية معلومات مفصلة عن جميع إجراءات جمع المعلومات الشخصية، ويتضمن ذلك:

- سبب جمع المعلومات
- طريقة وإجراء جمع المعلومات
- تفاصيل المعلومات المجموعة وتصنيفها
- الأنظمة التي سيتم تخزين تلك المعلومات بها، ويفضل تعريف نسخة موحدة عن كل نوع من المعلومات الشخصية على نظام موحد، ويتم نسخها أو جزء منها للأنظمة الأخرى عند الحاجة
- تعريف مالك محدد للمعلومة من قبل جهات العمل المختلفة داخل الجامعة. " Information Business Owner "
- تعريف مالك محدد للمعلومة من قبل تقنية المعلومات. " Information IT Owner "

جميع الأشكال التي يسمح للمعلومة باتخاذها، مثلاً:

قاعدة البيانات - ملف اكسل - ملف نصيCSV - دورة حياة المعلومة - من يحق له الوصول للمعلومة أو لجزء منها، وتعريف شكل الدخول - من يحق له التصريح بالحصول على المعلومة، وإجراءات إعطاء التصريح، وطرق توثيق ومراقبة وتدقيق تلك الإجراءات.

١٤ - بعد حصر المعلومات الشخصية وتوثيق جميع المعلومات والإجراءات المتعلقة بها في "دليل المعلومات الشخصية"، يجب على إدارة تقنية المعلومات إعادة تعريف وهيكلة إجراءات الحصول على المعلومات.

١٥ - إجراء الحصول على المعلومات الشخصية: يتم تعريف الإجراء عبر نموذج الكتروني بما يحقق التالي: يجب أن يذكر طلب الحصـــول على المعلومات الشـخصـــية جميع أشـــكال اســـتخدامها، وهل هو مؤقت أو دائم، مع تحديد وقت الانتهاء من الاستخدام

- يجب أن يتضمن النموذج معلومات تفصيلية عن المعلومات المطلوبة.
- يجب أن يتضمن النموذج طريقة الوصول للمعلومة، هل هو وصول للمعلومة عبر النظام، أو الحصول على نسخة منها.
- يجب أن يتضمن النموذج تعهداً بحذف المعلومات بعد انتهاء السبب من الحصول عليها.
- في حال الحصول على نسخة من المعلومة، يجب أن يعرف الطلب شكل الحصول على المعلومات.
- في حال طلب المعلومات الشخصية لمشاركتها مع طرفٍ ثالث، يجب أن يتضمن النموذج معلومات تفصيلية عن هذا الطرف.
- في حال مشـاركة المعلومة مع طرف ثالث أو أكثر، سـواءً أكان ذلك الطرف من داخل أو من خارج الجامعة، فإن على جميع الأطراف الطالبة للمعلومة الحرص على:
- تعبئة نموذج الحصول على المعلومات الشخصية.
- الموافقة الخطية على هذه الوثيقة في حال كان الطرف طالب المعلومات من خارج الجامعة، ويمكن أن تكون الموافقة عن طريق إرســـال بريد الكتروني يرســـل من عنوان الجهة الطالبة للمعلومة، ولا تقبل عناوين البريد الإلكتروني الشخصية.
- يجب أن يتضمن النموذج تعهداً من طالب المعلومة بالالتزام بالسياسة والإجراءات المتبعة.
- يجب أن يتضمن النموذج موافقة مسؤول حماية المعلومات الشخصية، وموافقة عميد تقنية المعلومات.

١٦ - يحق للجامعة اسـتخلاص البيانات الديموغرافية من المعلومات الشـخصـية، واسـتخدامها لإجراء العمليات الإحصـائية لأغراض البحث العلمي والتخطيط الإداري وذلك دون الرجوع للمسـتخدمين، وذلك بشـرط أن يتم حذف أي بيانات يمكن أن تؤدي لتمييز أو تعقب الأفراد.

١٧ - إن أي استخدام للبيانات الديموغرافية يجب ألا يتم إلا بعد:

- تعبئة طالب المعلومات لنموذج حصول على المعلومات.
- تسجيل الاستخدامات في "دليل المعلومات الشخصية."
- مراجعة مســـؤول حماية المعلومات الشـــخصـــية للبيانات المطلوبة، للتأكد من خلوها من بيانات تمييز أو تعقب الأفراد.
- موافقة مسؤول حماية المعلومات الشخصية وموافقة عميد تقنية المعلومات.

- في حال نشر أو مشاركة أي معلومات شخصية، فيجب الحصول على موافقة أصحاب المعلومات بشكل صريح قبل نشر المعلومات الشخصية.

١٨ - يجب أن يتاح لجميع المستخدمين إمكانية الدخول ومراجعة معلوماتهم الشخصية للتأكد من صحتها. ويجب أن يتاح لهم طريقة واضحة لتعديل هذه المعلومات سواءً بشكل مباشر أو بالرجوع لموظفي الجامعة

١٩ - يكون مسؤول حماية المعلومات الشخصية مسؤولاً عن تدقيق المعلومات بشكل دوري لضمان صحتها وتكاملها في حال وجودها على أكثر من نظام.

٢٠ - يجب التقليل ما أمكن من استخدام البيانات الشخصية في عمليات الاختبار والتطويرTesting and Development ، مع التوجيه الدائم باستخدام بيانات وهمية لمستخدمين وهميين ما أمكن ذلك في عمليات الاختبار المختلفة التي قد تقوم بها فرق تقنية المعلومات أو باقي فرق المنظمة.

٢١ - في حال استخدام المعلومات الشخصية لأغراض الاختبار والتطوير، فيجب أيضاً تعبئة النموذج الخاص بالحصول على المعلومات الشخصية.

٢٢ - يجب أن يتم تدريب موظفي تقنية المعلومات على التعامل بشكل خاص مع البيانات الشخصية للمستخدمين والحرص عليها، وأن يوافق المستخدمين بشكل صريح وخطي على سياسة التعامل مع البيانات الشخصية. وينطبق ذلك على جميع موظفي الجامعة الذين تتطلب طبيعة عملهم الوصول لهذه المعلومات بشكل مباشر أو غير مباشر.

٢٣ - يجب أن يتضمن التدريب على التعامل مع البيانات الشخصية، تدريب الموظفين على إجراءات إنشاء تنبيه في حالات حدوث أي اختراق للخصوصية.

٢٤ - تعريف إجراءات واضحة للتعامل مع حالات اختراقات الخصوصية، وذلك بحسب تصنيف المعلومات التي يشك بتسربها، على أن يتضمن ذلك: تاريخ ووقت الاختراق - فئات المستخدمين المتضررة - تقييم مدى الضرر والخطر الذي قد ينجم عنه - تبليغ أصحاب المعلومات بحدوث الاختراقات - إجراءات التصعيد التي يجب اتباعها.

٢٥ - يمكن مشاركة أي بيانات شخصية مع الجهات الحكومية الأخرى في المملكة العربية السعودية، وذلك عن طريق وجود خطاب رسمي بذلك.

٢٦ - تكون إدارة تقنية المعلومات مسؤولةً عن تعريف نموذج للتعهد بعدم إفشاء المعلومات، يتضمن المعلومات الشخصية بشكل صريح، ومتابعة الحصول على موافقة جميع الشركات والأفراد المتعاقدين بشكل خطي على هذا النموذج.

٢٧- يمكن للمواقع الإلكترونية التابعة للجامعة تسجيل معلومات عن المستخدمين وذلك عن طريق تقنية ال Cookies وذلك دون وجود موافقة صريحة من المستخدم، وإن أي استخدام للمواقع التابعة للجامعة، يعتبر موافقةً ضمنيةً على هذه السياسة، وعلى استخدام هذه التقنية.