ECU
EGYPTIAN CHINESE UNIVERSITY
الجامعة المصرية الصينية
EDUCATION NEW ERA

سياسة حماية البيانات الشخصية

سياسة حماية البيانات الشخصية

بيان السياسة

تلتزم الجامعة المصرية الصينية بحماية خصوصية وسرية وسلامة وأمن البيانات الشخصية المتعلقة بالطلاب، وأعضاء هيئة التدريس، والعاملين الإداريين، والباحثين، والخريجين، والشركاء، والزوار.

وتقوم الجامعة بمعالجة البيانات الشخصية بصورة قانونية وعادلة وشفافة وآمنة وفقًا لما يلي:

- قانون حماية البيانات الشخصية المصري رقم (١٥١) لسنة ٢٠٢٠.
- اللوائح والتشريعات المصرية المنظمة للتعليم العالي.
- أفضل الممارسات الدولية في مجال أمن المعلومات وحماية الخصوصية.
- المعايير الأخلاقية الحاكمة للعمليات الأكاديمية والإدارية.

الهدف

تهدف هذه السياسة إلى:

- حماية البيانات الشخصية والبيانات الحساسة التي تتعامل معها الجامعة المصرية الصينية.
- تحديد المسؤوليات المتعلقة بجمع البيانات وتخزينها ومعالجتها ونقلها والتخلص منها.
- ضمان الامتثال لتشريعات حماية البيانات المصرية.
- تعزيز الشفافية والثقة في عمليات الجامعة.
- الحد من المخاطر المرتبطة بالوصول غير المصرح به أو إساءة الاستخدام أو الإفصاح غير المشروع أو التهديدات السيبرانية.

نطاق التطبيق

تسري هذه السياسة على:

- جميع كليات الجامعة وإداراتها ومراكزها ووحداتها ومكاتبها الإدارية.
- جميع العاملين وأعضاء هيئة التدريس والطلاب والمتعاقدين والاستشاريين ومقدمي الخدمات من الأطراف الثالثة.
- جميع السجلات الورقية والإلكترونية التي تحتوي على بيانات شخصية.
- جميع الأنظمة والمواقع الإلكترونية والمنصات والتطبيقات وقواعد البيانات التابعة للجامعة.

التعريفات

البيانات الشخصية

أي معلومات تتعلق بشخص طبيعي يمكن التعرف عليه، بما في ذلك:

- الاسم.
- الرقم القومي أو رقم جواز السفر.
- الرقم الجامعي أو الرقم الوظيفي.
- رقم الهاتف.
- البريد الإلكتروني.

- السجلات الأكاديمية.
- المعلومات المالية.
- عنوان بروتوكول الإنترنت (IP Address) .
- البيانات البيومترية أو البيانات المتعلقة بالصحة.

البيانات الشخصية الحساسة

هي البيانات المتعلقة بما يلي:

- الحالة الصحية.
- البيانات البيومترية.
- المعتقدات الدينية.
- الوضع المالي.
- السجلات الجنائية.
- أي معلومات تتطلب حماية معززة بموجب القانون.

صاحب البيانات

أي شخص طبيعي يمكن التعرف عليه وتتم معالجة بياناته بواسطة الجامعة.

المعالجة

أي عملية تتم على البيانات الشخصية، بما في ذلك جمعها أو تسجيلها أو تخزينها أو استخدامها أو مشاركتها أو نقلها أو حذفها.

مبادئ حماية البيانات

تضمن الجامعة أن تكون البيانات الشخصية:

- معالجة بطريقة قانونية وعادلة.
- مجمعة لأغراض أكاديمية وإدارية مشروعة.
- مقتصرة على المعلومات الضرورية فقط.
- دقيقة ويتم تحديثها بانتظام.
- محفوظة بشكل آمن وسري.
- محتفظًا بها للمدة اللازمة فقط.
- محمية من الوصول غير المصرح به أو التعديل أو الإفصاح أو الإتلاف.

الأساس القانوني للمعالجة

تقوم الجامعة بمعالجة البيانات الشخصية في الحالات التالية:

- حصولها على موافقة صاحب البيانات.
- إذا كانت المعالجة ضرورية للإدارة الأكاديمية.
- إذا كانت المعالجة مطلوبة بموجب القانون أو من الجهات الحكومية المختصة.
- إذا كانت المعالجة ضرورية للوفاء بالالتزامات الوظيفية.
- إذا كانت المعالجة ضرورية لحماية المصالح الحيوية للأفراد.
- إذا كانت المعالجة تدعم الأغراض التعليمية والبحثية المشروعة.

حقوق أصحاب البيانات

يحق للأفراد الذين تتم معالجة بياناتهم بواسطة الجامعة ما يلي:

- الوصول إلى بياناتهم الشخصية.
- طلب تصحيح البيانات غير الدقيقة.
- سحب الموافقة متى كان ذلك ممكنًا قانونًا.
- طلب تقييد معالجة البيانات.
- طلب حذف البيانات في الحالات التي يجيزها القانون.
- معرفة كيفية استخدام بياناتهم.
- تقديم شكاوى بشأن إساءة استخدام بياناتهم الشخصية.

جمع البيانات واستخدامها

تقوم الجامعة بجمع البيانات الشخصية لأغراض تشمل:

- قبول الطلاب وتسجيلهم.
- إدارة السجلات الأكاديمية.
- إدارة الموارد البشرية.
- الأنشطة البحثية.
- إدارة الرسوم والمصروفات والشؤون المالية.
- خدمات المكتبة وأنظمة إدارة التعلم (LMS).
- الأمن والسلامة داخل الحرم الجامعي.
- الاتصالات والفعاليات الجامعية.
- عمليات الاعتماد وضمان الجودة.

ولا يجوز استخدام البيانات الشخصية لأغراض غير مرتبطة بهذه الأهداف دون مبرر قانوني مشروع.

تدابير أمن البيانات

تطبق الجامعة التدابير الفنية والتنظيمية المناسبة لحماية البيانات، بما في ذلك:

- الخوادم الآمنة وقواعد البيانات المشفرة.
- آليات التحكم في صلاحيات الوصول.
- حماية كلمات المرور والمصادقة متعددة العوامل.
- المراقبة الدورية للأمن السيبراني.
- إجراءات النسخ الاحتياطي.
- برامج التوعية والتدريب للعاملين.
- التخلص الآمن من السجلات ووسائط التخزين.

مشاركة البيانات والإفصاح عنها

يجوز للجامعة مشاركة البيانات الشخصية فقط في الحالات التالية:

- مع الجهات الحكومية المخولة قانونًا.

- مع الشركاء الأكاديميين أو البحثيين المعتمدين.
- مع مقدمي الخدمات بموجب اتفاقيات سرية المعلومات.
- عندما يقتضي القانون ذلك.
- بناءً على موافقة صريحة من صاحب البيانات.

ويُحظر تمامًا الإفصاح غير المصرح به عن البيانات الشخصية.

نقل البيانات خارج جمهورية مصر العربية

يجب أن يتم أي نقل للبيانات الشخصية خارج جمهورية مصر العربية وفقًا للقوانين المصرية السارية وبما يضمن توفير مستويات حماية مناسبة للبيانات.

إدارة حوادث اختراق البيانات

يجب الإبلاغ فورًا عن أي حادثة مشتبه بها أو مؤكدة تتعلق باختراق البيانات الشخصية إلى الجهة المختصة داخل الجامعة.

وتلتزم الجامعة بما يلي:

- التحقيق الفوري في الحوادث.
- الحد من المخاطر والأضرار الناتجة عنها.
- إخطار الجهات المختصة عند الضرورة.
- اتخاذ الإجراءات التصحيحية والوقائية اللازمة.

مدة الاحتفاظ بالبيانات

تلتزم الجامعة بالاحتفاظ بالبيانات الشخصية فقط للمدة اللازمة لتحقيق الأغراض التي جُمعت من أجلها أو وفقًا للمتطلبات القانونية والتنظيمية المعمول بها.

وتلتزم الجامعة بما يلي:

- تحديد فترات الاحتفاظ بالبيانات وفقًا لطبيعة البيانات والغرض من استخدامها.
- مراجعة البيانات المحفوظة بصورة دورية للتأكد من استمرار الحاجة إليها.
- حذف البيانات أو إتلافها أو إخفاء هويتها بصورة آمنة عند انتهاء فترة الاحتفاظ المقررة أو انتفاء الحاجة إليها.
- الاحتفاظ بالسجلات الأكاديمية والمالية والإدارية وفقًا للمدد المحددة في القوانين واللوائح المنظمة للتعليم العالي والجهات الرقابية المختصة.
- ضمان تطبيق إجراءات آمنة للتخلص من البيانات الورقية والإلكترونية بما يمنع استعادتها أو إساءة استخدامها.

فئة السجل	مدة الاحتفاظ
السجلات الأكاديمية وكشوف الدرجات والشهادات الجامعية للطلاب	بشكل دائم
طلبات الالتحاق للمتقدمين غير المقبولين	سنتان
السجلات التأديبية للطلاب	5 سنوات بعد التخرج أو الانفصال عن الجامعة
سجلات حضور الطلاب	5 سنوات
سجلات المساعدات والمنح المالية للطلاب	7 سنوات
السجلات الطبية للطلاب	7 سنوات بعد آخر قيد أو دراسة بالجامعة
ملفات العاملين وأعضاء هيئة التدريس	7 سنوات بعد انتهاء الخدمة

فئة السجل	مدة الاحتفاظ
سجلات الرواتب والضرائب	7 سنوات
سجلات التوظيف للمتقدمين غير المقبولين	سنتان
سجلات المشروعات البحثية	من 5 إلى 10 سنوات بعد انتهاء المشروع
موافقات وأخلاقيات البحث العلمي	10 سنوات
البيانات البحثية التي تتضمن بيانات شخصية	من 5 إلى 10 سنوات أو وفقًا لاشتراطات الجهة الممولة
السجلات المالية والمحاسبية	7 سنوات
سجلات المشتريات والعقود	7 سنوات بعد انتهاء العقد
تسجيلات كاميرات المراقبة (CCTV)	من 30 إلى 90 يومًا ما لم تكن مطلوبة للتحقيقات أو الإجراءات القانونية
سجلات الزوار	سنة واحدة
سجلات الدخول واستخدام الأنظمة الإلكترونية وتقنية المعلومات	من سنة إلى 3 سنوات
سجلات البريد الإلكتروني (المراسلات الإدارية العامة)	من 3 إلى 7 سنوات
سجلات استعارة المكتبة	حتى إعادة المواد المستعارة بالإضافة إلى سنة واحدة
بيانات التواصل الخاصة بالخريجين	حتى سحب الموافقة أو انتفاء الحاجة إليها
سجلات الاعتماد الأكاديمي وضمان الجودة	10 سنوات أو بشكل دائم للتقارير المؤسسية الرئيسية

مسؤول حماية البيانات

تقوم الجامعة بتعيين مسؤول لحماية البيانات أو جهة مختصة تتولى الإشراف على تطبيق متطلبات حماية البيانات الشخصية داخل الجامعة.

وتشمل مسؤوليات مسؤول حماية البيانات ما يلي:

- متابعة الالتزام بأحكام قانون حماية البيانات الشخصية المصري رقم (١٥١) لسنة ٢٠٢٠ والسياسات الداخلية ذات الصلة.
- تقديم المشورة والدعم للإدارات المختلفة بشأن حماية البيانات والخصوصية.
- مراقبة عمليات معالجة البيانات وتقييم المخاطر المرتبطة بها.
- تلقي الاستفسارات والشكاوى المتعلقة بالبيانات الشخصية والتعامل معها.
- التنسيق مع الجهات الرقابية والتنظيمية المختصة عند الحاجة.
- الإشراف على برامج التوعية والتدريب الخاصة بحماية البيانات وأمن المعلومات.
- متابعة الإبلاغ عن حوادث اختراق البيانات واتخاذ الإجراءات التصحيحية المناسبة.
- إعداد التقارير الدورية للإدارة العليا بشأن مستوى الامتثال ومخاطر حماية البيانات.

ويجوز التواصل مع مسؤول حماية البيانات من خلال القنوات الرسمية التي تحددها الجامعة للإبلاغ عن أي استفسارات أو طلبات أو شكاوى تتعلق بالبيانات الشخصية.

المسؤوليات

إدارة الجامعة

- ضمان الامتثال المؤسسي لهذه السياسة.
- تخصيص الموارد اللازمة لتطبيق تدابير حماية البيانات.

العاملون وأعضاء هيئة التدريس

- التعامل مع البيانات بمسؤولية وسرية.

- الالتزام بإجراءات الأمن والحماية المعتمدة بالجامعة.

الطلاب

- استخدام أنظمة الجامعة بصورة مسؤولة.
- حماية بيانات الدخول والمعلومات الشخصية الخاصة بهم.

إدارة تكنولوجيا المعلومات

- المحافظة على البنية التحتية للأمن السيبراني وحماية البيانات.
- مراقبة الأنظمة والاستجابة للتهديدات الأمنية.

مخالفات السياسة

يترتب على مخالفة هذه السياسة اتخاذ واحد أو أكثر من الإجراءات التالية:

- إجراءات تأديبية.
- تعليق أو إلغاء صلاحيات الوصول إلى الأنظمة.
- جزاءات إدارية.
- اتخاذ الإجراءات القانونية عند الاقتضاء.

المراجعة والتحديث

تُراجع السياسة مرة واحدة على الأقل سنويًا أو كلما صدرت تشريعات أو متطلبات تنظيمية جديدة.