سياسة الأمن الرقمي في المدرسة

المرجع NECC-AD/IT/POL/2026/001

الإصدار 1.0

عام

جدول المحتويات

1. نظرة عامة

تحدد هذه السياسة إطار الحوكمة الرقمية والأمن السيبراني واستخدام التكنولوجيا في مركز محمد بن راشد للتعليم الخاصة – بإدارة مركز نيوإنجلاند للأطفال. وتهدف إلى ضمان الامتثال لسياسة دائرة التعليم والمعرفة الخاصة بالمدارس الرقمية (الإصدار 1.1، سبتمبر 2024)، مع تكييفها بما يتناسب مع البرنامج التخصصي للمركز في تعليم الطلبة من ذوي اضطراب طيف التوحد.

كما يعكس هذا المستند التزام المركز بالسياسات الداخلية ذات الصلة ضمن إطار موحّد موجّه للاستخدام العام.

2. الغرض والأهداف

- ضمان الامتثال لمتطلبات دائرة التعليم والمعرفة التالية المتعلّقة بالسياسة الرقمية والأمن السيبراني وحماية البيانات
- تعزيز الاستخدام الآمن والأخلاقي للأدوات الرقمية في جميع أنحاء المؤسسة.
- إرساء إدارة واستخدام آمنين للبنية التحتية التقنية.
- دعم الثقافة الرقمية والشمول بما يتماشى مع الخطط التعليمية الفردية.
- دمج الكفاءات الرقمية ضمن البرامج التعليمية والعلاجية.
- حماية البيانات الرقمية وضمان سريتها وسلامتها.
- تحديد المساءلة المتعلّقة بالسلامة الرقمية واستخدام التكنولوجيا.
- توفير تدريب مستمر للحفاظ على الامتثال وتعزيز الكفاءة الرقمية.

3. نطاق العمل

تنطبق هذه السياسة على جميع الموظفين، والمتعاقدين، والطلبة (حسبما تقتضيه الحاجة)، والزوار في مركز محمد بن راشد للتعليم الخاص ممن لديهم صلاحية الوصول إلى الأنظمة الرقمية أو البيانات الخاصة بمركز نيو إنجلاند للأطفال – أبو ظبي. وتُطبّق التعديلات اللازمة لضمان توافقها مع الخصائص النمائية والمتطلبات العلاجية للطلبة من ذوي اضطراب طيف التوحد.

4. التعريفات

التكنولوجيا العلاجية	الأدوات الرقمية التي تدعم أهداف التعلم أو التواصل أو السلوك ضمن الخطط التربوية الفردية لكل طالب.
الحماية الرقمية	الأنظمة والإجراءات التي تهدف إلى حماية الفئات الطلابية الأكثر عرضة للمخاطر من الأذى عبر الإنترنت.
أصول المعلومات	البيانات الرقمية أو المادية التي تمثل قيمة مؤسسية.

5. القوانين واللوائح المعول بها

- السياسة الرقمية لدائرة التعليم والمعرفة الخاصة بالمدارس الرقمية الإصدار 1.1 (2024).
- المرسوم بقانون اتحادي رقم (45) لسنة 2021 بشأن حماية البيانات الشخصية.
- المرسوم بقانون اتحادي رقم (34) لسنة 2021 بشأن مكافحة الشائعات والجرائم الإلكترونية.
- معيار أبوظبي لأمن المعلومات الصحية والأمن السيبراني (حيثما ينطبق).
- سياسات دائرة التعليم والمعرفة الخاصة بالدمج، والحماية، وسلوك الطلبة.

6. المسؤوليات

- **المدير التنفيذي**: يعتمد هذه السياسة ويشرف على تنفيذها.
- **لجنة الرفاهية الرقمية:** تشرف على الاستراتيجية الرقمية والمراجعة السنوية للسياسة.
- **قسم تقنية المعلومات:** يتولى تنفيذ إجراءات الأمن السيبراني، وضوابط الوصول، ونسخ البيانات الاحتياطية.
- **الموظفون:** يلتزمون بإرشادات الاستخدام المسؤول وبروتوكولات الحماية.
- **أولياء الأمور:** يدعمون الممارسات الرقمية الآمنة في المنزل.
- **الطلبة:** يلتزمون بإرشادات السلامة الرقمية المعتمدة في المدرسة، حسبما تقتضيه الحاجة.

7. إطار السياسة الرقمية

7.1 الاستراتيجية الرقمية والإشراف

- قام المركز بتطوير استراتيجية رقمية تشمل البنية التحتية، والتدريب، وأهداف الدمج .
- يجري المركز مراجعات سنوية تتضمن تقييمات للمخاطر، ويسعى للحصول على ملاحظات أصحاب المصلحة.
- عيّن المركز مسؤولًا عن السلامة الرقمية للتنسيق والتواصل مع دائرة التعليم والمعرفة.

7.2 الكفاءات الرقمية

- حدّد المركز نواتج تعلم قابلة للتحقيق في مجال الثقافة الرقمية، بما يتناسب مع طبيعة الفئة الطلابية الفريدة التي يخدمها المركز.
- يسعى المركز إلى دمج التكنولوجيا المناسبة ضمن التعليم الفردي والتعليم الصفي.
- يوفر المركز تدريبًا لجميع الموظفين حول الأمن السيبراني والتعامل مع البيانات.
- يقدم المركز لأولياء الأمور محتوى توعويًا مناسبًا حول الأمن الرقمي، يتوافق مع احتياجات الفئة الطلابية التي يخدمها المركز.

7.3 الاستخدام المسؤول والحماية

- الحفاظ على سياسات منفصلة للاستخدام المسؤول تشمل الموظفين، والطلبة وأولياء الأمور، والزوار.
- يُحظر استخدام شبكات VPN غير المصرح بها داخل بيئة العمل الرقمية للمركز، كما يتم تنظيم السلوك عبر وسائل التواصل الاجتماعي من خلال سياسة واضحة وإجراءات موحدة للنشر.
- يجب أن يتوافق استخدام الذكاء الاصطناعي والمحتوى الرقمي مع قوانين حقوق النشر المعمول بها لتجنب الانتحال.
- يتم تسجيل جميع حوادث الأمن السيبراني الرقمية والتحقيق فيها.
- يقدم المركز برامج توعية بالسلامة عبر الإنترنت تتناسب مع الفئات العمرية المختلفة.

7.4 البنية التحتية الرقمية

- يتم تأمين أنظمة تقنية المعلومات في المركز من خلال المصادقة متعددة العوامل، والجدران النارية (جدران الحماية)، والتشفير، وأنظمة الكشف والاستجابة على الأجهزة والمراقبة المستمرة، واختبارات الاختراق الدورية، والتحديثات المنتظمة.
- قام المركز بتطبيق أنظمة منع فقدان البيانات، وحماية الأجهزة الطرفية، وإدارة أمن الوضع السحابي.
- يحتفظ المركز بخطة للاستجابة للحوادث والتعافي منها ويتم مراجعتها بانتظام.

7.5 حماية البيانات والخصوصية

- وضع المركز سياسة لحماية البيانات تحدد متطلبات الموافقة، والاحتفاظ بالبيانات، ومشاركتها.
- تتم مراجعة خطة حماية البيانات سنويًا لضمان الامتثال لقوانين البيانات في دولة الإمارات العربية المتحدة.
- يمارس المركز العناية الواجبة عند تقييم الموردين من الأطراف الثالثة، ويشترط توقيع اتفاقيات عدم الإفصاح، والالتزام التعاقدي بقوانين دولة الإمارات مع الجهات التي تتعامل مع البيانات الشخصية.

7.6 الاتصالات الرقمية

- يحصل المركز على موافقة خطية قبل استخدام أو نشر الوسائط الرقمية الخاصة بالطلبة.
- تم وضع قواعد واضحة لحسابات الموظفين الشخصية على وسائل التواصل الاجتماعي، وإبلاغها للموظفين وتطبيقها.
- يحظر المركز التواصل الخاص بين الموظفين والطلبة عبر القنوات الشخصية.
- يتم الحفاظ على موقع المدرسة الإلكتروني بما يتوافق مع متطلبات دائرة التعليم والمعرفة الخاصة بمحتوى المواقع الإلكترونية.

8. التنسيق بين الجهات

يتحمل مسؤول السلامة الرقمية مسؤولية هذه السياسة، وكذلك التنسيق مع المدير العالمي لأمن المعلومات، وذلك لضمان الامتثال لمتطلبات دائرة التعليم والمعرفة والتوافق مع سياسات مركز نيو إنجلاند للأطفال المعتمدة.

9. الامتثال للسياسة والمراجعة

- يُعد الالتزام بهذه السياسة إلزاميًا.
- قد يؤدي عدم الامتثال لهذه السياسة إلى اتخاذ إجراءات تصحيحية وفقًا للوائح دائرة التعليم والمعرفة والقوانين المعمول بها في دولة الإمارات العربية المتحدة.
- تتم مراجعة هذه السياسة وتحديثها سنويًا أو عند الحاجة خلال فترات أقصر، لضمان استمرار الامتثال للوائح دولة الإمارات العربية المتّحدة.

10. الموافقة النهائية

تم اعتماد هذه السياسة والموافقة عليها من قِبَل إدارة المركز، وتدخل حيّز التنفيذ اعتبارًا من تاريخ **19 فبراير 2026.**

نهاية السياسة