تاريخ السريان	العام الدراسي 25/2024 (الفصل الدراسي الأول)
يبدأ الامتثال من	العام الدراسي 26/2025 (الفصل الدراسي الأول)

سياسة المدارس

بشأن

الرقمية

المقدمة

إن القدرة على التعامل مع معطيات العالم الرقمي أمر ضروري لتمكين الطلبة من المشاركة بفعالية في التعليم وشؤون العمل والحياة المعاصرة. لذا، تقع على عاتق المدارس مسؤولية دمج تطوير المهارات الرقمية في كل جانب من جوانب التعليم والتعلم، والأهم من ذلك ضمان سلامة وأمان الطلبة أثناء تفاعلهم في الفضاء الرقمي. تحدد هذه السياسة المتطلبات الأساسية للمدارس لوضع وتنفيذ إستراتيجية رقمية، ودمج مفهوم الأمان الرقمي في عمليتي التعليم والتعلم والاستخدام الآمن للتكنولوجيا الرقمية.

الغرض

- تحديد متطلبات دائرة التعليم والمعرفة التي تقتضي أن تقوم المدارس بوضع وتنفيذ إستراتيجية رقمية تتعلق باستخدامها للتكنولوجيا والأهداف المتعلقة بالكفاءات الرقمية والبنية التحتية وتدابير الأمان الرقمي والموارد المطلوبة.
- ضمان استثمار المدارس في تطوير المهارات والكفاءات الرقمية للطلبة لتمكينهم من الاستفادة من فرص التعلم الناجمة عن استخدام التكنولوجيا.
- ضمان تثقيف المدارس للطلبة حول الوصول المسؤول والآمن واستخدام البيئات الرقمية وحماية الطلبة من المحتوى الرقمي والتفاعلات التي قد تكون غير لائقة أو ضارة.
- ضمان وضع المدارس لأنظمة وآليات وإجراءات آمنة ومتوازنة ومناسبة لحماية أمنها الرقمي.
- ضمان التزام المدارس بمتطلبات مركز المتابعة والتحكم والمرسوم بقانون اتحادي رقم (45) لعام 2021 بشأن حماية البيانات الشخصية في جمع ومعالجة وتخزين البيانات الشخصية.

التعريفات

الاحتياجات التعليمية الإضافية	المتطلبات الفردية للحصول على دعم إضافي أو تعديلات أو تسهيلات داخل البيئة المدرسية على أساس دائم أو مؤقت استجابة لسياق معين. ينطبق هذا على أي دعم يتطلبه الطلبة أصحاب الهمم وأولئك الذين لديهم احتياجات تعليمية خاصة و/أو عوائق إضافية أمام التعلم أو الوصول أو التفاعل في هذا السياق المحدد (على سبيل المثال، الأشخاص من ذوي عسر القراءة أو الإعاقة السمعية أو البصرية أو الطلبة الموهوبين ذوي الخصوصية المزدوجة أو الموهوبين و/ أو الفائقين). على سبيل المثال، قد يحتاج الطالب ذو الحركة المحدودة إلى مواءمة الدرس للمشاركة في حصص التربية الرياضية وإجراء التسهيلات للوصول إلى المرافق، لكنه قد لا يحتاج إلى أي مواءمة في التقييمات. وبالمثل، قد يحتاج الطالب ذو الإعاقة السمعية إلى دعم تقني إضافي في الفصل للوصول إلى محتوى الدرس، بالإضافة إلى تسهيلات مادية أخرى للوصول إلى المادة التعليمية (مثال: الجلوس في مقدمة الفصل للتمكن من قراءة الشفاه).
التكنولوجيا المساعدة	أي عنصر أو أداة أو برنامج أو نظام لمنتج يُستخدم لتعزيز القدرات الوظيفية للأشخاص ذوي الاحتياجات الخاصة والحفاظ عليها أو تحسينها (الرابطة الدولية للتكنولوجيا المساعدة، بدون تاريخ).
استخدام الأجهزة الشخصية في المدرسة (BYOD)	ممارسة تسمح المدارس من خلالها للموظفين و/أو الطلبة باستخدام أجهزتهم الرقمية الشخصية لأداء أعمالهم.
التنمر	هو الاعتداء الجسدي أو النفسي أو الاجتماعي أو اللفظي المتكرر الذي يمارسه الطلبة الذين يشعرون أنهم في موقع قوة ضد طلبة آخرين يُنظر إليهم على أنهم أضعف أو عاجزين بطريقة تؤذي الطالب جسدياً و/أو نفسياً وذلك لتحقيق مكاسب محددة أو لفت الانتباه. يمكن أن يرتكب التنمّر من قبل مجموعات أو أفراد، وذلك عبر الإنترنت (التنمّر الإلكتروني) أو في العالم الواقعي. توفر السياسة الوطنية للوقاية من التنمر في المؤسسات التعليمية (وزارة التربية والتعليم، غير مؤرخة) إطارًا شاملاً للتنمر والتنمر الإلكتروني.
التنمر الإلكتروني	التنمر الإلكتروني هو التنمّر التي يحدث عبر الإنترنت "باستخدام وسائل التواصل وتكنولوجيا المعلومات في إهانة شخص أو استخدام الألفاظ النابية تجاهه أو التهديد بالعنف أو تشويه السمعة أو الابتزاز" (وزارة التربية والتعليم، 2020). يمكن أن يتبع هذا النوع من التنمر الطالب أينما كان، وله مدى أوسع من التنمّر في العالم الواقعي وذلك عبر شبكات التواصل الاجتماعي والهواتف المحمولة، ويتميز بقدرته على الوصول لنطاق أوسع من التأثير مقارنة بالتنمر في البيئات الواقعية.

حوادث الأمن السيبراني	خرق يهدد سرية، أو سلامة، أو توافر نظم المعلومات، أو البيانات الحساسة في أي مؤسسة.
حماية البيانات	عملية حماية البيانات من التلف أو التسريب أو الوصول غير المصرح به أو الضياع بالإضافة إلى توفير القدرات اللازمة لاسترجاع البيانات وإعادتها إلى حالتها التشغيلية في حالة تعرضها للتلف أو الفقدان. (منظمة صناعات شبكات التخزين، غير مؤرخة).
الجهاز الرقمي	جهاز يستخدم للتواصل الصوتي أو عبر الفيديو أو النصي أو أي نوع آخر من الحواسيب أو أداة شبيهة بالحواسيب، على سبيل المثال لا الحصر الهواتف المحمولة والساعات الذكية والأجهزة اللوحية والحواسيب المحمولة.
الحادث الرقمي	واقعة يقوم بها أحد أفراد المجتمع المدرسي من خلال توظيف التكنولوجيا الرقمية بشكل غير لائق. تتضمن هذه الحوادث خرقاً لسياسات الاستخدام المقبول، أو الوصول إلى محتوى غير مناسب، أو السلوكيات أو التواصل غير اللائق والتنمر الإلكتروني و/أو أي انتهاكات أخرى للوائح المدرسية في البيئة الإلكترونية.
الإلمام بالعلوم الرقمية	الحالة التي يكون فيها الفرد مستخدمًا كفؤًا وواثقًا وآمناً ومسؤولاً ومبدعاً وحريصاً على استكشاف التكنولوجيا.
خطة التعلم الموثقة	خطة تحدد أهداف التعلم الشخصية والتعديلات في المنهج والدعم الإضافي أو الأدوات التعليمية التي يوافق عليها طاقم المدرسة وأولياء الأمور والطلبة (عند الضرورة)، بما في ذلك الخطط التعليمية الفردية (IEP) وخطط الدعم الفردي (ISP) وخطط التعلم الفردي (ILP) وخطط دعم السلوك (BSP) وخطط التعلم المتقدمة (ALP) وغير ذلك. قد تكون هذه الخطة لمعالجة أي حاجة أكاديمية أو سلوكية أو لغوية أو اجتماعية وعاطفية محددة.
ولي الأمر	الشخص المسؤول عن الطفل أو المُكلف برعايته بموجب القانون، والمعروف بالقائم على رعاية الطفل وفقًا للمرسوم بقانون اتحادي رقم 3 لسنة 2016 بشأن حقوق الطفل "وديمة".
المعلومات الشخصية	معلومات تتعلق بأفراد يمكنك من خلالها التعرف إليهم مباشرة أو يمكن التعرف عليهم بشكل غير مباشر من خلال تلك المعلومات بعد ربطها بمعلومات أخرى.
تقييم المخاطر	عملية منهجية لتقييم المخاطر المحتملة التي قد ينطوي عليها نشاط أو مسعى معين.

ضمان الرعاية	الجهود المبذولة لضمان أمان الطلبة من التعرض للأذى، شاملة الحماية من سوء المعاملة ومختلف المخاطر التي قد تؤثر على نموهم الشخصي والتعليمي وصحتهم ورفاهيتهم وأمنهم.
إدارة وضعية الأمان للبرمجيات كخدمة (SSPM)	أداة أمنية آلية متقدمة تعمل على رصد المخاطر الأمنية ضمن تطبيقات البرمجيات كخدمة (SaaS). كما تحدد الإعدادات غير المناسبة والحسابات غير الضرورية وصلاحيات المستخدم المفرطة ومخاطر عدم الامتثال بالإضافة إلى تقييم ومعالجة المشكلات الأمنية الأخرى المتعلقة بالتقنيات السحابية.
وسائل التواصل الاجتماعي	وسيلة للتفاعل الاجتماعي حيث يقوم الأشخاص بإنشاء و/أو مشاركة و/أو تبادل المعلومات والأفكار في المجتمعات الافتراضية والشبكات، على سبيل المثال لا الحصر منصات مثل فيسبوك وتويتر وإنستغرام ولينكد إن ويوتيوب.
الزائر	لأغراض هذه السياسة، الزائر هو أي شخص يأتي إلى مقر المدرسة بشكل مؤقت (أحد أولياء الأمور أو قريب لطالب، طالب محتمل وأولياء أموره، مفتشون، مقاولون وغير ذلك). الزائر المدعو هو أي شخص يزور المدرسة بشكل مؤقت للتفاعل مع الطلبة (متحدث، ممثل في معرض وظيفي وغير ذلك) ويشمل المتطوعين الذين يشاركون من قبل مؤسسة تعليمية على أساس غير مدفوع للتفاعل مع الطلبة (مرافقي الطالب وغير ذلك).

السياسة

1. الوثائق المطلوبة

1.1 يتعين على المدارس إعداد وتنفيذ الوثائق التالية، ونشرها على موقع المدرسة الإلكتروني باللغة العربية والإنجليزية أو بلغة التدريس المعتمدة، بما يتوافق مع متطلبات هذه السياسة:

1. الإستراتيجية الرقمية (انظر القسم 2.1 الإستراتيجية الرقمية).
2. سياسات الاستخدام المسؤول (انظر القسم 4.1 سياسات الاستخدام المسؤول).
3. إطار عمل لاختيار الموردين والمنتجات الخارجية (انظر القسم 5.5 مقدمو الخدمات والمنتجات الخارجيون).
4. البيانات والبنية التحتية للأمن السيبراني (انظر القسم 6.1 البنية التحتية الآمنة لتكنولوجيا المعلومات).
5. خطة الاستجابة فيما يتعلق بحوادث الأمن السيبراني (انظر القسم 6.6 حوادث الخرق الأمني السيبراني).
6. خطة حماية بيانات المدرسة والسياسة المتعلقة بها (انظر القسم 7. حماية البيانات).
7. سياسة الوسائط الرقمية وسياسة وسائل التواصل الاجتماعي (انظر القسم 8. الاتصالات الرقمية).

2. الإستراتيجية الرقمية والرقابة

2.1 الإستراتيجية الرقمية: يجب على المدارس وضع وتنفيذ إستراتيجية رقمية تحدد وتبرر الأهداف الرقمية لمدة خمس سنوات. ويجب أن تتضمن الإستراتيجية:

1. توجه إستراتيجي شامل حول كيفية استخدام التكنولوجيا لتحسين الإنجازات التعليمية للطلبة والمخرجات (لتعزيز التدريس والتعلم ودعم الإدارة المدرسية بكفاءة وفعالية على سبيل المثال).
2. تقييم كيف يمكن للمدرسة استخدام وتوفير التكنولوجيا المساعدة لتمكين الدمج.
3. أهداف متعلقة بمهارات وكفاءات الطلبة الرقمية اللازمة للتعلم.

4. خطط التطوير والشراء والتنفيذ للبنية التحتية الرقمية والبرمجيات والأجهزة.

5. آليات لضمان أمن النظم الرقمية للمدرسة.

6. خطة لتحديث البنية التحتية الرقمية للمدرسة، حيثما كان ذلك ممكناً.

7. الموارد والاستثمارات المطلوبة لتنفيذ الإستراتيجية الرقمية.

8. متطلبات تدريب الكادر التعليمي والإداري.

9. تعزيز الوعي بالتكنولوجيات الحديثة الناشئة (مثل الذكاء الاصطناعي).

2.2 الرقابة: يتولى مسؤول أو لجنة الإشراف الرقمي المسؤوليات التالية فيما يخص الرقابة على إستراتيجية المدرسة الرقمية والسياسات المصاحبة لها:

1. وضع وتنفيذ إستراتيجية المدرسة الرقمية.

2. إجراء مراجعة سنوية للإستراتيجية الرقمية وطرق تنفيذها:
   أ. رصد التقدم المحقق نحو تحقيق أهداف التعليم للطلبة وخطط التطوير وخطط الشراء في المدرسة.
   ب. فحص التقنيات، والبرامج، والمنصات الإلكترونية للتأكد من مطابقتها لأهداف الإستراتيجية.
   ج. اختبار وتقييم المخاطر للأنظمة والبنية التحتية الرقمية للمدرسة (مثل النسخ الاحتياطي والاسترداد) للتحقق من أمانها وأنها تلبي الغرض المنشود.
   د. مراجعة كفاءة تدابير المدرسة لحماية البيانات والأمان السيبراني.
   هـ. إعادة تقييم احتياجات المدرسة التكنولوجية بناءً على آراء الموظفين وأولياء الأمور والطلبة وتخطيط الشراء والتطوير الرقمي وفقًا لذلك.
   و. إعادة النظر في احتياجات التطوير الرقمي للموظفين وتحديد الدورات التدريبية الإضافية اللازمة.

3. وضع وتطبيق ومراجعة سياسات المدرسة الأخرى المطلوبة وفقاً لهذه السياسة.

4. التواصل مع الشركاء المعنيين (مثل الموظف المسؤول عن الشؤون الرقمية أو رئيس قسم تكنولوجيا المعلومات) للاسترشاد بقراراتهم.

2.3 ينبغي للمدارس تعيين أحد الموظفين للتنسيق مع دائرة التعليم والمعرفة بشأن المسائل المتعلقة بالكفاءة والأمان الرقمي.

3. الكفاءات الرقمية

3.1 المخرجات التعليمية: يجب على المدارس تحديد الكفاءات الرقمية والنتائج المتوقعة من الطلبة حسب الصف/السنة ودمجها في منهاج المدرسة. يجب على المدارس التأكد من أن لديها البنية التحتية الرقمية المناسبة والموارد اللازمة لدعم الطلبة في تحقيق هذه النتائج، بما في ذلك الطلبة الذين يحتاجون إلى دعم تعليمي إضافي وفقًا *لسياسة دائرة التعليم والمعرفة للدمج في المدارس*.

3.2 تدريب الموظفين: يجب على المدارس توفير تدريب ذي صلة للموظفين وفقاً لمسمياتهم الوظيفية لتمكينهم من تعزيز أهداف هذه السياسة. يجب أن يغطي التدريب موضوعات مثل البنية التحتية الرقمية للمدرسة والسياسات ونتائج التعلم الرقمي للطلبة وحماية البيانات والأمن السيبراني وتدابير السلامة الرقمية التي تنفذها المدرسة. الاستخدام المسؤول والحماية الرقمية

4. الاستخدام المسؤول والحماية الرقمية

4.1 سياسات الاستخدام المسؤول: ينبغي للمدارس أن تصمم وتعمم سياسات للاستخدام الرقمي الرشيد التي تستهدف الطلبة وأولياء الأمور والموظفين والزوار. يجب على هذه السياسات تحديد الأنشطة المسموح بها/ المنوعة لهذه المجموعات داخل الحرم المدرسي وعلى شبكتها وأنظمتها الرقمية، ويجب أن تشمل:

1. تعريف الاستخدام المسؤول لبرمجيات المدرسة وشبكتها وخدماتها والأجهزة الرقمية التي توفرها المدرسة بما في ذلك الأجهزة المشتركة.

2. قواعد الاستخدام المسموح بها والمحظورة بالنسبة للأجهزة الشخصية على شبكة المدرسة وداخل حرمها، وأثناء الأنشطة اللاصفية التي تقام خارج المدرسة (مثل الرحلات الميدانية).
   أ. يجب على المدارس تقييد استخدام الشبكات الافتراضية الخاصة (VPNs) من قبل الطلبة داخل حرم المدرسة أو عبر شبكات المدرسة ما لم يُصرح بذلك صراحةً لأغراض تعليمية أو إدارية محددة.

3. معايير فيما يتعلق باستخدام حسابات وسائل التواصل الاجتماعي الشخصية من قبل الموظفين (انظر القسم 8.3 حسابات الموظفين الشخصية على منصات التواصل الاجتماعي).

4. قوانين المدرسة فيما يتعلق بإنشاء ومشاركة كلمات السر لحسابات المدرسة.

5. المعايير الخاصة بمشاركة البيانات المتعلقة بالمدرسة أو المجتمع المدرسي، والقنوات التي يمكن من خلالها مشاركة هذه البيانات عند السماح بذلك. يتضمن ذلك معايير تتعلق برفع بيانات الطلبة على تطبيقات خارجية وأدوات تعليمية حيثما كان ذلك ممكنًا.

6. معايير فيما يتعلق بالأمانة الأكاديمية والسرقة الفكرية والاستخدام المسؤول للمواد المحفوظة بحقوق النسخ والنشر والأدوات الرقمية (مثل الذكاء الاصطناعي)، وفقًا للمرسوم بقانون اتحادي رقم (38) لعام 2021 بشأن حقوق المؤلف والحقوق المجاورة وشروط وأحكام دائرة التعليم والمعرفة وسياسة حقوق النسخ والنشر وسياسة خصوصية البيانات فيما يتعلق بجمع المعلومات واستخدامها والإفصاح عنها.

7. يجب على المدارس تعميم سياسات الاستخدام المسؤول ذات الصلة على الطلبة وأولياء الأمور والموظفين والزوار عبر قنوات مناسبة.
   أ. يجب على المدارس نشر سياسات الاستخدام المسؤول المطبقة على الطلبة وأولياء الأمور على موقع المدرسة الإلكتروني وفي دليل أولياء الأمور وفقاً *لسياسة دائرة التعليم والمعرفة لمشاركة أولياء الأمور في المدارس*.
   ب. يتعين على المدارس إعداد نسخ من السياسة ملائمة لأعمار الطلبة حتى الصف السادس/السنة السابعة، وتوفير النسخة الكاملة من السياسة لأولياء الأمور.

4.2 حماية الطلبة: يجب على المدارس وضع برامج تعليمية وأنظمة فعّالة لحماية الطلبة من المخاطر الإلكترونية المذكورة أدناه.

1. المخاطر الإلكترونية التي قد تواجه الطلبة:
   أ. التعرض لمحتوى غير مناسب أو غير قانوني أو محتوى قد يضر بصحتهم النفسية.
   ب. التعرض لتواصل إلكتروني غير آمن (مثل التواصل مع مستخدمين لديهم ملفات شخصية مزيفة).
   ج. سلوك شخصي على الإنترنت قد يؤدي إلى الإضرار بالنفس أو بالآخرين (مثل المشاركة في التنمر الإلكتروني).
   د. الاحتيال والمخاطر المالية مثل المقامرة والتصيد الإلكتروني.

2. يجب على المدارس وضع البرامج والأنظمة والآليات والإجراءات التالية لحماية الطلبة من المخاطر الإلكترونية وضمان سلامتهم المتكاملة:

أ. برنامج توعية مناسب لجميع الطلبة من كافّة الأعمار ويغطي فوائد التكنولوجيا ويعزز الوعي بالمخاطر الإلكترونية وتأثير العادات الرقمية على أمنهم وسلامتهم (مثل تأثير مدة استخدام الأجهزة الرقمية).

ب. أنظمة تصفية (فلترة) ومتابعة مناسبة لمراقبة استخدام الطلبة للإنترنت على أجهزة وأنظمة المدرسة.

ج. تحليل دوري لاستخدام الطلبة للإنترنت وانتهاكات الشبكة الإلكترونية لتحديد الاتجاهات السلبية المحتملة أو المشكلات.

د. إجراءات لتحديد ودعم الطلبة الذين يبدو أنهم يطورون عادات رقمية محفوفة بالمخاطر أو مفرطة أو غير قانونية، مثل الإدمان الرقمي أو القمار، وفقًا *لسياسة دائرة التعليم والمعرفة للصحة النفسية للطلبة في المدارس وسياسة دائرة التعليم والمعرفة لسلوك الطلبة في المدارس*.

هـ. آليات لتمكين الحماية خلال الأنشطة التي تُجرى افتراضيًا (مثل تعطيل الدردشة الخاصة بالطلبة).

3. يجب على المدارس التأكد من وجود غرض تطويري قبل السماح للطلبة باستخدام الإنترنت خلال ساعات الدراسة.

4.3 الحوادث الرقمية:

1. تقع الحادثة الرقمية عندما يقوم أحد أفراد مجتمع المدرسة باستخدام التكنولوجيا الرقمية بشكل غير مناسب. يشمل ذلك خرق سياسات الاستخدام المعقول والوصول إلى محتوى غير مناسب والسلوكيات غير اللائقة أو التواصل غير المناسب أو التنمر الإلكتروني أو أي خرق آخر للوائح المدرسة في بيئة الإنترنت.

2. عندما تقع حادثة رقمية خلال ساعات الدراسة أو في أوساط تسري عليها سياسات المدرسة الرقمية، يجب على المدارس إجراء تدخلات وتقديم الدعم للطلبة و/أو الموظفين وفقًا للسياسة ذات الصلة (مثل *سياسة دائرة التعليم والمعرفة للتوظيف في المدارس*، *وسياسة دائرة التعليم والمعرفة للسلامة التكاملة للموظفين في المدارس*، *وسياسة دائرة التعليم والمعرفة للشؤون الإدارية للطلبة في المدارس*، *وسياسة دائرة التعليم والمعرفة لمشاركة أولياء الأمور في المدارس*، *وسياسة دائرة التعليم والمعرفة لسلوك الطلبة في المدارس*، *وسياسة دائرة التعليم والمعرفة لحماية الطلبة في المدارس*). يجب على المدارس إبلاغ دائرة التعليم والمعرفة عن الحوادث الرقمية والتعاون مع شرطة أبوظبي في التحقيقات عند الضرورة.

3. يجب على المدارس التأكد من تسجيل كل حادثة رقمية وتوثيقها وتوقيعها من قبل المدير وحفظها لأغراض التدقيق وفقًا *لسياسة دائرة التعليم والمعرفة للسجلات في المدارس*.

4.4 يجب على المدارس مطالبة أولياء الأمور بمراقبة استخدام أبنائهم للأجهزة الرقمية خارج حرم المدرسة وخارج ساعات الدراسة لضمان السلوك الرقمي الآمن والمناسب.

5. البنية التحتية الرقمية

5.1 الأجهزة الرقمية: يجب على المدارس التأكد من أن الأجهزة الرقمية الممنوحة لأفراد المدرسة تتمتع بميزات أمان مناسبة. في حال السماح للموظفين بالوصول إلى بيانات أو أنظمة المدرسة على أجهزة أخرى أو وجود سياسة استخدام الجهاز الشخصي (BYOD) للموظفين أو الطلبة، يجب على المدرسة تحديد وتنفيذ تدابير الأمان الرقمي (مثل الحد الأدنى لمواصفات الجهاز ومتطلبات مكافحة الفيروسات).

5.2 الأنظمة الرقمية للموظفين: يجب على المدارس التأكد من إمكانية وصول أعضاء الهيئة المعنيين إلى الأنظمة الرقمية التي توفرها دائرة التعليم والمعرفة بما في ذلك نظام إدارة التعلم.

5.3 جاهزية تطبيق التعلم عن بُعد: يجب على المدارس تبني تدابير للتعلم عن بُعد في حالات الطوارئ مثل إغلاق المدارس مؤقتاً أو لبعض الطلبة الذين لديهم ظروف استثنائية (مثل البقاء في المستشفى لفترات طويلة أو السفر الطارئ مع أولياء الأمور لفترات طويلة).

5.4 التكنولوجيا المساندة: يجب على المدارس توفير التكنولوجيا المساندة للطلبة الذين لديهم احتياجات تعليمية إضافية كما هو موضح في خطة التعلم الموثقة الخاصة بهم وفقاً *لسياسة دائرة التعليم والمعرفة للدمج في المدارس*.

5.5 مقدمو الخدمات والمنتجات الخارجيون:

1. يجب على المدارس وضع إطار لتقييم المخاطر المتعلقة بالأطراف الثالثة لاختيار مقدمي خدمات تكنولوجيا المعلومات الخارجيين والمنتجات المتعلقة بشبكة المدرسة ونظامها وبنيتها التحتية بما في ذلك مقدمو تطبيقات التعلم والتطبيقات مفتوحة المصدر. يجب أن يشتمل هذا الإطار على ما يلي على الأقل:
    أ. التوافق مع أنظمة المدرسة الحالية.
    ب. إدارة آمنة للبيانات.
    ج. الامتثال لمعايير وأطر عمل الأمن السيبراني.
    د. الأمان ضد التهديدات السيبرانية.
    هـ. توفير الخدمات وتدابير النسخ الاحتياطي/الاسترداد.
    و. سمعة مزود الخدمة واستقراره المالي.
    ز. التزام المورد بالمرسوم بقانون اتحادي رقم (45) لعام 2021 بشأن حماية البيانات الشخصية وشروط وأحكام دائرة التعليم والمعرفة وسياسة حقوق النسخ والنشر وسياسة خصوصية البيانات الخاصة بجمع المعلومات واستخدامها والإفصاح عنها.
    ح. عند اللزوم (مثل مقدمي تطبيقات التعلم) الجودة التعليمية وملاءمة العمر للمحتوى.

2. يجب على المدارس إبلاغ الموردين الخارجيين بأن المورد خاضع للمرسوم بقانون اتحادي رقم (45) لعام 2021 بشأن حماية البيانات الشخصية وشروط وأحكام دائرة التعليم والمعرفة وسياسة حقوق النسخ والنشر وسياسة خصوصية البيانات الخاصة بجمع المعلومات واستخدامها والإفصاح عنها.

6. البيانات والأمن السيبراني

6.1 البنية الرقمية الآمنة لتكنولوجيا المعلومات: يجب على المدارس إنشاء بنية تحتية رقمية آمنة وقوية وضمان تطبيق الضوابط الأمنية السيبرانية ذات الصلة كما يلي:

1. التحكم في الوصول/ الدخول
   أ. تطبيق آليات المصادقة متعددة العوامل بالنسبة للخدمات بالغة الأهمية.
   ب. تعريف وتطبيق نظام التحكم في الوصول بناءً على الدور لضمان حصول المستخدمين على التصاريح المناسبة.

2. تشفير البيانات
   أ. تطبيق التشفير على البيانات المنقولة والمخزنة لحماية المعلومات الحساسة.

3. أمان الشبكات
   أ. استخدام جدران الحماية الحديثة (نظام أمان) وأنظمة كشف/منع التسلل للحماية ضد الوصول غير المصرح به.
   ب. التأكد من تنفيذ سياسات تصفية (فلترة) الشبكة.
   ج. التأكد من القدرة على حجب المحتوى غير المناسب.
   د. القدرة على كشف الأجهزة المتأثرة/ المصابة عبر شبكة المدرسة.
   هـ. التأكد من تطبيق جدران الحماية (نظام أمان) القائمة على الهوية لتوفير رؤية تفصيلية لنشاط تصفح المستخدمين.
   و. إنشاء بنية أمنية موحدة لجميع متصفحات الإنترنت.
   ز. مراقبة وتدقيق حركة الشبكة بانتظام لاكتشاف الأنماط غير المعتادة.

4. حماية نقاط النهاية (Endpoint)
   أ. تثبيت وتحديث برمجيات مكافحة الفيروسات/البرامج الضارة على جميع الأجهزة التي تديرها المدرسة.
   ب. تنفيذ تشفير القرص الصلب والتأكد من التحديث الأمني المنتظم.

5. النسخ الاحتياطي للبيانات والاسترجاع
   أ. إنشاء إجراءات نسخ احتياطي منتظمة وآلية للبيانات ذات الأهمية.
   ب. التأكد من أن النسخ الاحتياطية مؤمنة ومخزنة بعيدًا عن الشبكة.
   ج. تطوير خطة استرجاع قوية في حال وقوع حادث أمني لتقليل وقت تعطل الخدمة.

6. أمان البيانات
   أ. إنشاء ضوابط تصنيف البيانات الخاصة ببيانات المدرسة والطلبة.
   ب. تطبيق أدوات منع فقدان البيانات لضمان عدم تسرب البيانات أو اختراقها.

7. التدريب لتعزيز الوعي الأمني
   أ. إجراء جلسات تدريب منتظمة للموظفين والطلبة لتعزيز الوعي حول تهديدات الأمان السيبراني وأفضل الممارسات.

8. خطة الاستجابة للحوادث
   أ. وضع وتحديث خطة استجابة الحوادث بشكل منتظم لمعالجة الخروقات الأمنية بشكل فوري وفعّال.
   ب. إجراء محاكاة لهجوم سيبراني والتدرب بمشاركة إدارة المدرسة.

9. الأمن الحسي
   أ. التأكد من تأمين الوصول إلى الخوادم ومعدات الشبكة والبنية التحتية المهمة الأخرى.

10. الامتثال التنظيمي
   أ. التأكد من الامتثال للوائح والمعايير الدولية والمحلية لحماية البيانات.

11. المراقبة والسجلات
   أ. تنفيذ أنظمة مراقبة شاملة لاكتشاف الحوادث الأمنية والاستجابة لها في الوقت الفعلي.
   ب. الاحتفاظ بسجلات مفصلة لأغراض التدقيق والتحليل.

12. تطوير البرمجيات الآمن
   أ. اتباع ممارسات البرمجة الآمنة عند تطوير أو شراء البرمجيات التعليمية.
   ب. تحديث البرمجيات بانتظام وتصحيح الثغرات الأمنية.

13. الأمن السحابي (الحوسبة السحابية)
   أ. يجب التأكد من التزام المزودين المختارين بمعايير أمان صارمة في حال استخدام الخدمات السحابية.
   ب. تطبيق ضوابط تهيئة ووصول مناسبة لموارد الخدمات السحابية.

ج. دمج الخدمات السحابية – البرمجيات بوصفها مع خدمات الهوية المدرسية حيثما أمكن.

د. إنشاء قدرات إدارة الوضعية الأمنية للبرمجيات كخدمة سحابية(SaaS).

14. أمن منصات التعاونات

أ. تأمين منصات التواصل والتعاون لحماية المعلومات التعليمية الحساسة المشتركة بين الطلبة والموظفين.

15. أمن الأطراف الثالثة

أ. فحص ومراقبة موردي التكنولوجيا التعليمية من الأطراف الثالثة لضمان تلبيتهم لمعايير الأمان.

6.2 صيانة النظام: يجب على المدارس الحفاظ على بنيتها التحتية الرقمية وأنظمة التشغيل والأنظمة الأمنية والبرمجيات، بما في ذلك برمجيات الحماية من الفيروسات وتحديثها بانتظام. يجب على المدارس اختبار بنيتها التحتية وأنظمتها الرقمية بانتظام لضمان أنها تعمل بشكل جيد.

6.3 الاستخدام الآمن لتطبيقات التعلم الخارجية: يجب أن تتوفر لدى المدارس آليات حماية (مثل أنظمة الدخول الموحد) لحماية أمن الطلبة والنظام عند استخدام تطبيقات التعلم الخارجية.

6.4 التواصل الافتراضي الآمن مع الزوار: يجب على المدارس طلب موافقة أولياء الأمور لأي تواصل افتراضي مباشر مع الزوار سواء داخل الصف أو خارجه. يجب أن تتم الموافقة على جميع هذه التفاعلات أيضاً من قبل دائرة التعليم والمعرفة وفقاً لسياسة دائرة التعليم والمعرفة للأنشطة اللاصفية والفعاليات في المدارس وسياسة دائرة التعليم والمعرفة لحماية الطلبة في المدارس.

6.5 النسخ الاحتياطي والتخزين: يجب على المدارس التي لديها أنظمة تخزين بيانات ضمان إجراء نسخ احتياطية للمعلومات المهمة والبرمجيات وإعدادات التهيئة بما يتماشى مع سياسة دائرة التعليم والمعرفة للسجلات في المدارس فيما يتعلق بعدد المرات والمدة الزمنية المناسبة.

1. يجب على المدارس التأكد من أن هذه النسخ الاحتياطية مخزنة بشكل آمن ومنفصل عن شبكة المدرسة.

2. يجب على المدارس التي تستخدم الأنظمة السحابية الخارجية للتخزين التأكد من مزامنة بياناتها مع السحابة.

6.6 حوادث الخرق الأمني السيبراني: يجب على المدارس وضع خطط الاستجابة واستمرارية الأعمال لإرشاد الموظفين في حال وقوع خرق أمني سيبراني، بما في ذلك بروتوكولات الإبلاغ عن الحادث لإدارة المدرسة ولدائرة التعليم والمعرفة وعملية الحفاظ على الاستمرارية التشغيلية.

1. يجب على المدارس عدم التبليغ بأي حادث خرق سيبراني للأطراف الخارجية باستثناء مزود الخدمة المعني ودائرة التعليم والمعرفة.

2. يجب على المدارس الالتزام بجميع القوانين والسياسات المعمول بها من قبل دائرة التمكين الحكومي وأي سلطات أخرى ذات صلة في الإمارات العربية المتحدة، بما في ذلك المرسوم بقانون اتحادي رقم (34) لعام 2021 بشأن مكافحة الشائعات والجرائم الإلكترونية.

7. حماية البيانات

7.1 سياسة حماية البيانات: يجب على المدارس وضع سياسة حماية بيانات تحدد كيف ستضمن المدرسة التعامل مع المعلومات الشخصية بطريقة صحيحة وآمنة والامتثال للمرسوم بقانون اتحادي رقم (45) لعام 2021 بشأن حماية البيانات الشخصية والتي يجب أن تشمل على الأقل:

1. تحديد أنواع المعلومات الشخصية التي يمكن جمعها.

2. المتطلبات والإجراءات لموافقة الفرد على جمع ومعالجة وتخزين المعلومات الشخصية.
   أ. يجب أن يتم منح الموافقة بحرية تامة ويجب أن تكون محددة ومدروسة وواضحة.
   ب. يمكن للفرد سحب الموافقة في أي وقت.

3. الظروف التي يمكن بموجبها مشاركة المعلومات الشخصية من قبل المدرسة مع أفراد أو جهات أخرى (مثل دائرة التعليم والمعرفة).
   أ. يجب أن تتضمن المدارس اتفاقية عدم إفصاح مدمجة في أي عقود مع المقاولين يُحظر بموجبها مشاركة البيانات الشخصية داخل الدولة أو خارجها لأي غرض دون موافقة صريحة من دائرة التعليم والمعرفة.

7.2 مشاركة البيانات مع دائرة التعليم والمعرفة: يجب على المدارس تقديم بيانات دقيقة ومحدثة لموظفي دائرة التعليم والمعرفة المخولين عند الطلب، وفقًا للمرسوم بقانون اتحادي رقم (18) لسنة 2020 بشأن التعليم الخاص وتعديلاته والقانون رقم (9) لعام 2018 بشأن إنشاء دائرة التعليم والمعرفة ووفقاً لشروط وأحكام دائرة التعليم والمعرفة، وسياسة خصوصية البيانات بالنسبة لجمع واستخدام والإفصاح عن المعلومات.

1. يجب على المدارس إبلاغ أولياء الأمور بالتزاماتهم بمشاركة البيانات مع دائرة التعليم والمعرفة وفقًا لذلك.

7.3 خطة حماية البيانات: يجب على المدارس وضع ومراجعة خطة حماية البيانات سنويًا، بما يتوافق مع المرسوم بقانون اتحادي رقم (45) لعام 2021 بشأن حماية البيانات الشخصية *وسياسة دائرة التعليم والمعرفة للسجلات في المدارس*. يجب أن تحدد خطة حماية البيانات الخطوات التي اتخذتها المدرسة لحماية بياناتها التنظيمية بما في ذلك طرق تصنيف البيانات ومستويات التفويض والحماية ضد التهديدات السيبرانية وغيرها من التهديدات وإجراءات استعادة المعلومات المدعومة في حالات الخرق.

8. الاتصالات الرقمية

8.1 سياسة الوسائط الرقمية: يجب على المدارس وضع وتنفيذ ومراقبة سياسة الوسائط الرقمية التي تحكم إنشاء ونشر الوسائط الرقمية. يجب أن تتضمن السياسة على الأقل:

1. متطلبات الحصول على موافقة قبل التسجيل والنشر الرقمي:
   أ. يجب على المدارس أخذ الصور الفوتوغرافية و/أو تسجيلات الفيديو للطلبة بعد الحصول على موافقة خطية من أولياء الأمور. بعد الحصول على الموافقة، يجب على المدارس إبلاغ أولياء الأمور بالغرض من التقاط الصور و/أو تسجيلات الفيديو.
   ب. يجب على المدارس الحصول على موافقة خطية من أولياء الأمور قبل نشر المحتوى الرقمي الذي يتضمن الطلبة. يجب على المدارس أن تحدد بوضوح ما إذا كان سيتم تعريف الطالب بالاسم في النشر عند الحصول على الموافقة.
2. إجراءات تقديم وسحب الموافقة.
3. الشروط المتعلقة بتخزين وأمن الوسائط الرقمية.
4. الشروط المتعلقة باستخدام الأجهزة الشخصية والحسابات لتسجيل أو نشر محتوى المدرسة.

8.2 سياسة وسائل التواصل الاجتماعي: يجب على المدارس وضع وتنفيذ سياسة وسائل التواصل الاجتماعي فيما يتعلق باستخدام وسائل التواصل الاجتماعي من قبل المدرسة.

1. يجب أن تتضمن السياسة، على الأقل:
   أ. منصات وحسابات وسائل التواصل الاجتماعي التي ستستخدمها المدرسة.
   ب. إجراءات الوصول والأمان وحماية كلمات المرور لحسابات وسائل التواصل الاجتماعي للمدرسة.
   ج. الشروط المتعلقة بالمحتوى واستخدام اللغة والتفاعل مع الحسابات الأخرى.

د. الشروط المتعلقة باستخدام الأسماء والصور ومقاطع الفيديو للطلبة وفقًا للقسم 8.1 سياسة الوسائط الرقمية.

هـ. إرشادات المنسقين (انظر القسم 8.2.3 المنسقون) فيما يتعلق بالمحتوى الذي تنشره الأطراف الثالثة على صفحات وسائل التواصل الاجتماعي للمدرسة، بما في ذلك إجراءات إدارة المحتوى غير اللائق والتصيد.

و. إجراءات التعامل مع السلوكيات السلبية الأخرى على وسائل التواصل الاجتماعي مثل تقليد حسابات المدرسة.

2. مراقبة الاتصالات المدرسية: يجب على المدارس مراقبة جميع قنوات الاتصال المدرسية الرسمية وغير الرسمية (النشرات الإخبارية، وسائل التواصل الاجتماعي، مجموعات تواصل أولياء الأمور، وغيرها) بانتظام لضمان التزامها بهذه السياسة.

3. المنسقون: يجب على المدارس تعيين منسق(ين) للموافقة المسبقة على المحتوى الذي ينشره مستخدمون آخرون على صفحات وسائل التواصل الاجتماعي للمدارس أو إزالته حيثما أمكن وفقًا لإرشادات المدرسة. يجب على المنسق(ين) رفض أو إزالة المحتوى الذي لا يتوافق مع القيم الثقافية في الإمارات العربية المتحدة أو يرقى إلى التنمر أو التحرش أو التمييز أو الترهيب، وفقاً *لسياسة دائرة التعليم والمعرفة للقيم وقواعد الأخلاق في المدارس وسياسة دائرة التعليم والمعرفة للاعتبارات الثقافية في المدارس*.

8.3 حسابات الموظفين الشخصية على منصات التواصل الاجتماعي: يجب على المدارس السماح لأعضاء هيئة التدريس بإنشاء حسابات شخصية على منصات التواصل الاجتماعي والحفاظ على القائم منها. فيما يتعلق بهذه الحسابات، يجب على الموظفين:

1. عدم استخدام عناوين البريد الإلكتروني الصادرة عن المدرسة لإنشاء مثل هذه الحسابات.

2. استخدام أعلى إعدادات الخصوصية الممكنة.

3. عدم التعريف بأنفسهم كمنتسبين للمدرسة، باستثناء على منصات التواصل الاجتماعي المهنية (مثل LinkedIn).

4. عدم قبول دعوات للتواصل أو المتابعة من الطلبة الحاليين أو السابقين دون سن 18 عاماً، أو إرسال مثل هذه الطلبات.

5. عدم قبول دعوات من أولياء أمور الطلبة الحاليين للتواصل أو المتابعة.

6. عدم استخدام هذه الحسابات للتواصل مع الطلبة الحاليين أو أولياء أمورهم أو الطلبة السابقين دون سن 18 عامًا. ينطبق هذا على تطبيقات المراسلة (مثل WhatsApp، Telegram، Signal).

7. الافتراض أن المحتوى المنشور من خلال هذه الحسابات (بما في ذلك المراجعات والتعليقات عبر الإنترنت) مرئي وقابل للبحث علناً بغض النظر عن إعدادات الخصوصية مع مراعاة حسن التصرف.

8. التأكد من أن المحتوى المشترك من خلال هذه الحسابات مناسب ويتوافق مع *سياسة دائرة التعليم والمعرفة للاعتبارات الثقافية في المدارس* ولا يصل إلى مستوى التنمر أو التحرش أو التمييز أو الترهيب وفقاً *لسياسة دائرة التعليم والمعرفة للقيم وقواعد الأخلاق في المدارس*.

9. التأكد من أن المحتوى المشترك من خلال هذه الحسابات لا يعطي الانطباع بأنه معتمد من قبل المدرسة.

10. التأكد من عدم مشاركة أي معلومات سرية تتعلق بالمدرسة من خلال هذه الحسابات.

8.4 الاتصالات عبر البريد الإلكتروني: يجب على المدارس إبلاغ أعضاء هيئة التدريس بأنهم غير مخولين باستخدام عناوين البريد الإلكتروني الشخصية للتواصل مع الطلبة أو أولياء الأمور.

8.5 موقع المدرسة الإلكتروني: يجب على المدارس إنشاء موقع إلكتروني مخصص لها وتحديثه باستمرار ليكون مرجعاً لأعضاء المجتمع المدرسي.

1. يجب على المدارس نشر المحتوى التالي على موقعها الإلكتروني على الأقل:
   أ. معلومات التواصل.
   ب. الخدمات التي تقدمها المدرسة.
   ج. الرسوم، بما في ذلك رسوم المواصلات ورسوم الأنشطة الاختيارية.
   د. تقارير التفتيش.
   هـ. بيانات إنجازات الطلبة الجماعية أو الإنجازات الفردية (مثل الجوائز)، ويتم ذلك بعد الحصول على الموافقة.

2. النسخ العامة من التقرير السنوي وفقاً *لسياسة دائرة التعليم والمعرفة للتقارير في المدارس*.
   أ. سياسات المدرسة ذات الصلة بأولياء الأمور و/أو الطلبة.
   ب. أي محتوى آخر مطلوب، كما هو محدد بواسطة سياسات دائرة التعليم والمعرفة.

3. يجب على المدارس التأكد من أن المحتوى المنشور على موقعها الإلكتروني دقيق ومناسب وفقاً *لسياسة دائرة التعليم والمعرفة للقيم وقواعد الأخلاق في المدارس*.

4. يجب على المدارس التأكد من أن المحتوى المنشور على موقعها الإلكتروني يتوافق مع متطلبات الوسائط الرقمية (انظر القسم 8.1 سياسة الوسائط الرقمية).

9. الامتثال

9.1 تعتبر هذه السياسة سارية اعتباراً من بداية العام الدراسي 25/2024 (الفصل الدراسي الأول). ومن المتوقع أن تكون المدارس متوافقة بالكامل مع هذه السياسة بحلول بداية العام الدراسي 26/2025 (الفصل الدراسي الأول).

9.2 عدم الامتثال لهذه السياسة سيعرض المدرسة للمساءلة القانونية والعقوبات المطبقة بموجب اللوائح والسياسات والمتطلبات الخاصة بدائرة التعليم والمعرفة، دون الإخلال بالعقوبات التي يفرضها المرسوم بقانون اتحادي رقم (31) لسنة 2021 بإصدار قانون الجرائم والعقوبات وتعديلاته أو أي قانون آخر ذي صلة. تحتفظ دائرة التعليم والمعرفة بحق التدخل إذا تبين مخالفة المدرسة لالتزاماتها.

المراجع

- دائرة التعليم والمعرفة في أبوظبي. (غير مؤرخ). شروط الاستخدام وبيان خصوصية المعلومات.
- جمعية صناعة التكنولوجيا المساعدة (ATIA). (غير مؤرخ). ما هي التكنولوجيا المساعدة؟
- المرسوم بقانون اتحادي رقم (3) لسنة 2016 بشأن حقوق الطفل "وديمة".
- المرسوم بقانون اتحادي رقم (18) لسنة 2020 بشأن التعليم الخاص وتعديلاته.
- المرسوم بقانون اتحادي رقم (31) لسنة 2021 بإصدار قانون الجرائم والعقوبات وتعديلاته.
- المرسوم بقانون اتحادي رقم (34) لسنة 2021 بشأن مكافحة الشائعات والجرائم الإلكترونية.
- المرسوم بقانون اتحادي رقم (38) لسنة 2021 بشأن حقوق المؤلف والحقوق المجاورة.
- المرسوم بقانون اتحادي رقم (45) لسنة 2021 بشأن حماية البيانات الشخصية.
- (IBM). (غير مؤرخ). ما هي الاستجابة للحوادث؟
- القانون رقم (9) لسنة 2018 بشأن إنشاء دائرة التعليم والمعرفة.
- وزارة التربية والتعليم. (2020). إدارة سلوك الطلبة بشأن التعلم عن بعد.
- وزارة التربية والتعليم. (2022). الميثاق المهني والأخلاقي للعاملين في مؤسسات التعليم العام
- وزارة التربية والتعليم. (غير مؤرخ). السياسة الوطنية لمحاربة التنمر في المؤسسات التعليمية.
- منظمة صناعات شبكات التخزين (SNIA) (غير مؤرخ). ما هي حماية البيانات؟
- جامعة تافتس. (غير مؤرخ). نظرة عامة على وسائل التواصل الاجتماعي.

النشر

2024 (سبتمبر). سياسة دائرة التعليم والمعرفة الرقمية في المدارس_الإصدار 1.1.

دائرة التعليم والمعرفة، أبوظبي

تطبق هذه السياسة على المدارس الخاصة ومدارس الشراكات التعليمية في أبوظبي، إلا أنه وفي حال وجود أي تعميم صادر قبل نشر هذه السياسة أو تم إصداره خصيصاً لمدارس الشراكات التعليمية فيما بعد فإنه يحل محل هذه السياسة.

الإصدارات السابقة:

2024 (يناير) سياسة دائرة التعليم والمعرفة الرقمية في المدارس_ الإصدار 1.0