مايو 2024/25(فصل الخريف)	فعالة من
مايو 2025/26(فصل الخريف)	الامتثال من

السياسة الرقمية

مقدمة

تعد القدرة على العمل في الفضاء الرقمي أمرًا لا غنى عنه للطلاب للمشاركة بشكل هادف في التعليم والعمل والحياة اليوم. وبالتالي، تتحمل المدارس مسؤولية دمج تنمية المهارات الرقمية في كل جانب من جوانب التدريس والتعلم، والأهم من ذلك في ضمان سلامة وأمن الطلاب أثناء مشاركتهم في الفضاء الرقمي. تحدد هذه السياسة المتطلبات الأساسية للمدارس في تطوير وتنفيذ الإستراتيجية الرقمية، وتوفير التعليم والتعلم بشأن السلامة الرقمية، واستخدامها الآمن للتكنولوجيا الرقمية.

غاية

•تحديد متطلبات دائرة التعليم والمعرفة بأن تقوم المدارس بتطوير وتنفيذ استراتيجية رقمية فيما يتعلق باستخدامها للتكنولوجيا، والأهداف المتعلقة بالكفاءات الرقمية والبنية التحتية، وتدابير الأمن الرقمي، والمطلوبة

موارد.

•التأكد من أن المدارس تستثمر في تطوير المهارات والكفاءات الرقمية لدى الطلاب لتمكينهم من تعظيم فرص التعلم التي يوفرها استخدام التكنولوجيا.

•التأكد من أن المدارس تقوم بتثقيف الطلاب حول الوصول والاستخدام المسؤول والآمن لبيئة الإنترنت وحماية الطلاب من المحتوى الرقمي والتفاعلات غير المناسبة أو الضارة.

•التأكد من قيام المدارس بوضع أنظمة وآليات وإجراءات آمنة ومتوازنة ومناسبة لحماية أمنها الرقمي.

•التأكد من التزام المدارس بمتطلبات المراقبة و
مركز التحكم والمرسوم بقانون اتحادي رقم (45)لسنة 2021في شأن حماية البيانات الشخصية في جمع ومعالجة وتخزين البيانات الشخصية.

تعريفات

التعلم الإضافي الاحتياجات	المتطلبات الفردية للحصول على دعم إضافي أو تعديلات أو تسهيلات داخل بيئة مدرسية على أساس دائم أو مؤقت استجابة لسياق معين. ينطبق هذا على أي دعم يطلبه الطلاب أصحاب الهمم وأولئك الذين لديهم احتياجات تعليمية خاصة و/أو حواجز إضافية أمام التعلم أو الوصول أو التفاعل في هذا السياق المحدد (على سبيل المثال، الذين يعانون من عسر القراءة، أو السمع أو ضعاف البصر، أو الاستثنائيين، أو الموهوبين و/ أو الموهوب). على سبيل المثال، قد يحتاج الطالب ذو الحركة المحدودة إلى تسهيلات في الدرس للمشاركة في التربية البدنية وبناء تسهيلات للوصول إلى المرافق ولكن قد لا يحتاج إلى أي تسهيلات في التقييمات. وبالمثل، قد يحتاج الطالب الذي يعاني من ضعف السمع إلى تكنولوجيا تكيفية ومساعدة للوصول إلى المحتوى في الفصل وقد يحتاج أيضًا إلى تسهيلات بدنية (على سبيل المثال، الجلوس في مقدمة الفصل لتتمكن من قراءة الشفاه) للوصول إلى التعلم.
	أي عنصر أو قطعة من المعدات أو برنامج أو نظام منتج يتم استخدامه لزيادة أو الحفاظ على أو تحسين القدرات الوظيفية للأشخاص ذوي الإعاقة .(ATIA، nd)
	الممارسة التي تسمح فيها المدارس للموظفين و/أو الطلاب بالقيام بعملهم على الأجهزة الرقمية المملوكة لهم شخصيًا.
تنمر	الاعتداء الجسدي أو الاجتماعي أو اللفظي المتكرر الذي يمارسه الطلاب الذين يشعرون أنهم في موقع قوة ضد الطلاب الآخرين الذين يُنظر إليهم على أنهم أضعف أو عاجزون، لتحقيق مكاسب محددة أو لفت الانتباه، بطريقة تؤذي الطالب جسديًا و/أو عاطفيًا . يمكن أن يتم ارتكاب التنمر من قبل مجموعات أو أفراد، عبر الإنترنت (التسلط عبر الإنترنت) أو عبر الإنترنت. توفر السياسة الوطنية لمنع التنمر في المؤسسات التعليمية (وزارة التربية والتعليم، الثانية) إطارًا كاملاً للتنمر والتسلط عبر الإنترنت.
التنمر الإلكتروني	التنمر الذي يحدث عبر الإنترنت. يمكن للتنمر عبر الإنترنت أن يتتبع الطالب الذي تعرض للتنمر أينما ذهب عبر شبكات التواصل الاجتماعي والهواتف المحمولة ويصل إلى نطاق أوسع من التنمر في العالم الحقيقي.
	خرق يهدد سرية أو سلامة أو توفر أنظمة معلومات المنظمة أو البيانات الحساسة .(IBM، nd)
حماية البيانات	عملية حماية البيانات من الفساد أو التسوية أو الوصول غير المصرح به أو الفقد وتوفير القدرة على استعادة البيانات إلى حالة وظيفية في حالة حدوث شيء يجعل البيانات غير قابلة للوصول أو غير قابلة للاستخدام .(SNIA، nd)
جهاز رقمي	جهاز يستخدم للاتصال الصوتي أو المرئي أو النصي أو أي نوع آخر من أجهزة الكمبيوتر أو الأجهزة الشبيهة بالكمبيوتر، بما في ذلك، على سبيل المثال لا الحصر، الهواتف المحمولة والساعات الذكية والأجهزة اللوحية وأجهزة الكمبيوتر المحمولة.

حادثة رقمية	مثال حيث يشارك أحد أعضاء المجتمع المدرسي في الاستخدام غير المناسب للتكنولوجيا الرقمية. يتضمن ذلك انتهاك سياسات الاستخدام المعقول، والوصول إلى محتوى غير مناسب، وسلوكيات أو اتصالات غير مناسبة، والتسلط عبر الإنترنت، و/أو أي خرق آخر للوائح المدرسة في بيئة عبر الإنترنت.
الطلاقة الرقمية	حالة كونك مستخدمًا كفؤًا وواثقًا وآمنًا ومسؤولًا ومبدعًا وفضوليًا للتكنولوجيا.
موثقة خطة التعلم	خطة تحدد أي أهداف تعليمية مخصصة، أو تعديلات على المناهج الدراسية، أو دعم إضافي، أو أدوات للتعلم يتم الاتفاق عليها من قبل موظفي المدرسة وأولياء الأمور والطلاب (عند الاقتضاء)، بما في ذلك الخطط التعليمية الفردية (IEP)، وخطط الدعم الفردي (ISP) ، وخطط التعلم الفردية (ILP)، وخطط دعم السلوك (BSP)، وخطط التعلم المتقدمة (ALP)، وما إلى ذلك. وقد يكون هذا لمعالجة أي احتياجات أكاديمية أو سلوكية أو لغوية أو اجتماعية وعاطفية محددة.
الأبوين	الشخص المسؤول قانوناً عن الطفل أو المكلف برعايته، ويعرف بأنه حاضن الطفل وفقاً للمرسوم بقانون اتحادي رقم (3)لسنة 2016في شأن حقوق الطفل.
شخصي معلومة	المعلومات المتعلقة بالأفراد الذين يمكن التعرف عليهم مباشرة من المعلومات المعنية، أو الذين يمكن التعرف عليهم بشكل غير مباشر من تلك المعلومات مع معلومات أخرى.
تقييم المخاطر	عملية منهجية لتقييم المخاطر المحتملة التي قد ينطوي عليها نشاط أو مشروع ما.
الحماية	حماية الطلاب من مخاطر الأذى، بما في ذلك سوء المعاملة وأنواع المخاطر الأخرى التي تؤثر على صحتهم ونموهم ورفاهيتهم وسلامتهم بشكل عام.
الأمن SaaS وضعية إدارة (SSPM)	نوع من أدوات الأمان الآلية لمراقبة المخاطر الأمنية في تطبيقات البرامج كخدمة (SaaS). كما أنه يحدد أيضًا التكوينات الخاطئة وحسابات المستخدمين غير الضرورية وأذونات المستخدم الزائدة ومخاطر الامتثال ومشكلات أمان السحابة الأخرى.
وسائل التواصل الاجتماعي	وسيلة للتفاعل الاجتماعي يقوم الأشخاص من خلالها بإنشاء و/أو مشاركة و/أو تبادل المعلومات والأفكار في المجتمعات والشبكات الافتراضية، بما في ذلك، على سبيل المثال لا الحصر، منصات مثل Twitterو Facebookو margatsnIو YouTubeو LinkedInو(جامعة تافتس، .(nd)
زائر	ولأغراض هذه السياسة، الزائر هو أي زائر مؤقت (على سبيل المثال، أحد الوالدين أو أحد أقارب الطالب، والطالب المحتمل وأولياء أمورهم، والمفتشين، والمقاولين، وما إلى ذلك) الذين يدخلون إلى مبنى المدرسة. الزائر المدعو هو أي شخص يزور المدرسة بشكل مؤقت للتفاعل مع الطلاب (على سبيل المثال، متحدث، ممثل معرض التوظيف، وما إلى ذلك) ويشمل المتطوعين الذين يتم تعيينهم من قبل مؤسسة تعليمية على أساس غير مدفوع الأجر للتفاعل مع الطلاب (على سبيل المثال، مرافقي الوالدين، وما إلى ذلك).

سياسة

1. الوثائق المطلوبة

1.1 يجب على المدارس تطوير وتنفيذ الوثائق التالية وإتاحتها على موقع مدرستها باللغتين العربية والإنجليزية أو لغة التدريس الخاصة بها، بما يتماشى 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 اختيار مقدمي الخدمات والمنتجات الخارجية (انظر القسم 5.4 مقدمي الخدمات والمنتجات الخارجية).
4. البيانات والأمن السيبراني (انظر القسم 6.1 هندسة تكنولوجيا المعلومات الرقمية الآمنة).
5. خطة الاستجابة فيما يتعلق بحوادث الأمن السيبراني (انظر القسم 6.6 حوادث الأمن السيبراني).
6. خطة وسياسة حماية بيانات المدرسة (انظر القسم 7. حماية البيانات).
7. سياسة الإعلام الرقمي وسياسة وسائل التواصل الاجتماعي (انظر القسم 8. الاتصالات الرقمية).

2. الاستراتيجية الرقمية والرقابة

2.1 الإستراتيجية الرقمية: يجب على المدارس تطوير وتنفيذ إستراتيجية رقمية تحدد أهدافها الرقمية وتوفر الأساس المنطقي لها خلال إطار زمني مدته 5 سنوات. يجب أن تشمل الإستراتيجية ما يلي:

1. التوجه الاستراتيجي العام حول كيفية نشر التكنولوجيا لتحقيق إنجازات ونتائج أفضل للطلاب (على سبيل المثال، لتعزيز التدريس والتعلم ودعم الإدارة بكفاءة وفعالية لإدارة المدرسة).
2. تقييم كيفية استخدام المدرسة للتكنولوجيا المساعدة وتوفيرها لتمكين الدمج.
3. الأهداف المرتبطة بمهارات الطالب الرقمية وكفاياته التي تمكنه من التعلم.
4. خطط التطوير والمشتريات والتنفيذ للبنية التحتية الرقمية والبرمجيات والأجهزة.
5. آليات ضمان أمن الأنظمة الرقمية للمدرسة.
6. التخطيط لتأمين البنية التحتية الرقمية للمدرسة في المستقبل، حيثما ينطبق ذلك.
7. الموارد والاستثمارات اللازمة لتنفيذ الاستراتيجية الرقمية.
8. متطلبات تدريب الموظفين.

.9زيادة الوعي المتعلق بالتقنيات الناشئة (على سبيل المثال، الاصطناعي
ذكاء).

2.2الإشراف: يجب أن يكون لدى لجنة الرفاهية الرقمية أو القائد ما يلي
المسؤوليات فيما يتعلق بالإشراف على الإستراتيجية الرقمية للمدرسة والسياسات المرتبطة بها:

.1تطوير وتنفيذ الإستراتيجية الرقمية للمدرسة.

.2إجراء مراجعة سنوية للاستراتيجية الرقمية وتنفيذها:
أ. مراقبة التقدم المحرز في تحقيق أهداف تعلم الطلاب وتطوير المدرسة
وخطط المشتريات.
ب. قم بتقييم التكنولوجيا والبرمجيات والمنصات عبر الإنترنت للتأكد من أنها
تحقيق أهداف الاستراتيجية.
ج. اختبار وإجراء تقييمات المخاطر للأنظمة الرقمية للمدرسة و
البنية التحتية (على سبيل المثال، استعادة النسخ الاحتياطي) للتأكد من أنها آمنة ومناسبة للغرض.

د. مراجعة مدى فعالية بيانات المدرسة والأمن السيبراني
أحكام.
ه. إعادة تقييم الاحتياجات التكنولوجية للمدرسة بناءً على تعليقات الموظفين وأولياء الأمور والطلاب، وتخطيط المشتريات والتطوير الرقمي
وفقًا لذلك.

.Fإعادة تقييم احتياجات التطوير الرقمي للموظفين وتحديد الاحتياجات الإضافية
التدريب مطلوب.

.3تطوير وتنفيذ ومراجعة السياسات المدرسية الأخرى المطلوب إنشاؤها بما يتماشى مع هذه السياسة.

.4الانخراط مع أصحاب المصلحة المعنيين (على سبيل المثال، المسؤول الرقمي، رئيس قسم تكنولوجيا المعلومات) لإبلاغ قراراته.

2.3يجب على المدارس تعيين أحد أعضاء هيئة التدريس للتواصل مع دائرة التعليم والمعرفة في الأمور المتعلقة بالكفاءة الرقمية والسلامة والأمن.

3.الكفاءات الرقمية

3.1نتائج الطلاب: يجب على المدارس تحديد الكفاءات الرقمية والنتائج المتوقعة للطلاب حسب الصف/السنة ودمجها في المنهج الدراسي للمدرسة. يجب على المدارس التأكد من أن لديها البنية التحتية والموارد الرقمية المناسبة لدعم الطلاب في تحقيق هذه النتائج، بما في ذلك الطلاب ذوي الاحتياجات التعليمية الإضافية، بما يتماشى مع سياسة الدمج الخاصة بدائرة التعليم والمعرفة.

3.2تدريب الموظفين: يجب على المدارس توفير التدريب المناسب للموظفين بما يتماشى مع متطلباتهم
التعيين لتمكينهم من تعزيز أهداف هذه السياسة. ويجب أن يغطي التدريب موضوعات مثل البنية التحتية الرقمية للمدرسة وسياساتها، ونتائج التعلم الرقمي
للطلاب، وحماية البيانات، والأمن السيبراني، وتدابير السلامة الرقمية التي تنفذها المدرسة.

4.الاستخدام المسؤول والحماية الرقمية

4.1سياسات الاستخدام المسؤول: يجب على المدارس تطوير ونشر المعلومات المسؤولة
سياسات الاستخدام الرقمي للطلاب وأولياء الأمور والموظفين والزوار. يجب أن تحدد هذه السياسات ما يُسمح/يحظر على هذه المجموعات القيام به في مباني المدرسة وشبكتها وأنظمتها، ويجب أن تشمل ما يلي:

.1تعريف الاستخدام المسؤول لبرامج المدرسة والشبكات والخدمات والأجهزة الرقمية الصادرة عن المدرسة، بما في ذلك الأجهزة المشتركة.

.2قواعد الاستخدام المسموح به والمقيد للأجهزة الشخصية على شبكة المدرسة ومباني المدرسة، وأثناء الأنشطة اللامنهجية التي تتم خارج المدرسة (على سبيل المثال، الرحلات الميدانية).

أ. يجب على المدارس تقييد استخدام الشبكات الافتراضية الخاصة (VPN)من خلال
الطلاب في مباني المدرسة أو من خلال شبكات المدارس ما لم يتم التصريح بذلك صراحةً لأغراض تعليمية أو إدارية محددة.

.3المعايير المتعلقة باستخدام حسابات وسائل التواصل الاجتماعي الشخصية من قبل الموظفين (انظر القسم .8.3حسابات وسائل التواصل الاجتماعي الشخصية للموظفين).

.4قواعد المدرسة فيما يتعلق بإعداد ومشاركة كلمات المرور الخاصة بالجهاز
حسابات المدرسة.

.5المعايير المتعلقة بمشاركة البيانات المتعلقة بالمدرسة أو المجتمع المدرسي، والقنوات التي يمكن من خلالها مشاركة هذه البيانات عندما يسمح بذلك. ويشمل ذلك المعايير المتعلقة بتحميل بيانات الطلاب على التطبيقات الخارجية وأدوات التعلم، حيثما ينطبق ذلك.

.6معايير الأمانة الأكاديمية، والانتحال، والمسؤول
استخدام المواد والأدوات الرقمية المحمية بحقوق النشر (مثل الذكاء الاصطناعي)، بما يتماشى مع المرسوم بقانون اتحادي رقم (38)لسنة 2021 في شأن حقوق المؤلف والحقوق المجاورة وشروط وأحكام دائرة التعليم والمعرفة، وسياسة حقوق النشر، وسياسة خصوصية البيانات فيما يتعلق في جمع المعلومات واستخدامها والكشف عنها.

.7يجب على المدارس توصيل سياسات الاستخدام المسؤول ذات الصلة للطلاب وأولياء الأمور والموظفين والزوار عبر القنوات المناسبة.

أ. يجب على المدارس نشر سياسات الاستخدام المسؤولة المطبقة على الطلاب وأولياء الأمور على موقع المدرسة وفي دليل أولياء الأمور، وفقًا لسياسة مشاركة أولياء الأمور الخاصة بدائرة التعليم والمعرفة.

ب. بالنسبة لجميع الطلاب الأصغر سنًا حتى الصف السادس/الصف السابع، يجب على المدارس توفير نسخ مناسبة من السياسة للطلاب، ونسخة كاملة من السياسة لأولياء الأمور.

4.2حماية الطلاب: يجب على المدارس وضع برامج تعليمية وأنظمة فعالة لحماية الطلاب من المخاطر عبر الإنترنت المذكورة أدناه.

.1المخاطر التي يتعرض لها الطلاب عبر الإنترنت هي كما يلي:
أ. التعرض لمحتوى غير لائق أو غير قانوني أو قد يضر بهم
الرفاهية.

ب. التعرض لتفاعلات غير آمنة عبر الإنترنت (على سبيل المثال، التفاعل مع المستخدمين ذوي الملفات الشخصية المزيفة).
ج. السلوك الشخصي عبر الإنترنت الذي يمكن أن يؤدي إلى إيذاء النفس أو الآخرين (على سبيل المثال، الانخراط في التسلط عبر الإنترنت). د. عمليات الاحتيال والمخاطر المتعلقة بالتمويل مثل المقامرة والتصيد الاحتيالي.

.2يجب على المدارس وضع البرامج والأنظمة والآليات والإجراءات التالية لحماية الطلاب من مخاطر الإنترنت وتعزيز رفاهيتهم: أ. برنامج توعية مناسب لعمر جميع الطلاب، يغطي فوائد التكنولوجيا، والوعي بمخاطر الإنترنت، والتقييم الذاتي للمخاطر عبر الإنترنت عند استخدام التكنولوجيا، وتدابير السلامة عبر الإنترنت، وتأثير العادات الرقمية على الرفاهية (على سبيل المثال، تأثير المدة استخدام الأجهزة الرقمية).

ب. أنظمة تصفية ومراقبة مناسبة لمراقبة الإنترنت لدى الطلاب
استخدامها على الأجهزة والأنظمة المدرسية.
ج. التحليل المنتظم لاستخدام الطلاب للإنترنت وانتهاكات مرشح الويب لتحديد الاتجاهات أو المشكلات السلبية المحتملة.

د. إجراءات تحديد ودعم الطلاب الذين يبدو أنهم كذلك
تطوير عادات رقمية خطيرة أو مفرطة أو غير قانونية، مثل الإدمان الرقمي أو المقامرة، بما يتماشى مع سياسة الصحة العقلية للطلاب في دائرة التعليم والمعرفة
وسياسة سلوك الطلاب الخاصة بدائرة التعليم والمعرفة.
ه. آليات لتمكين الحماية أثناء الأنشطة التي تتم افتراضيًا
(على سبيل المثال، تعطيل الدردشة الخاصة للطلاب).

.3يجب على المدارس التأكد من وجود غرض تنموي قبل السماح بذلك
-استخدام الطلاب للإنترنت أثناء ساعات الدراسة.

4.3الحوادث الرقمية:

.1تحدث حادثة رقمية عندما ينخرط أحد أعضاء المجتمع المدرسي في استخدام غير مناسب للتكنولوجيا الرقمية. يتضمن ذلك انتهاك سياسات الاستخدام المعقول، أو الوصول إلى محتوى غير مناسب، أو سلوكيات أو اتصالات غير مناسبة، أو التسلط عبر الإنترنت، أو أي خرق آخر للوائح المدرسة في بيئة عبر الإنترنت.

.2عندما تقع حادثة رقمية أثناء ساعات الدراسة أو في الأماكن التي يتم تغطيتها
السياسات الرقمية للمدارس، يجب على المدارس القيام بالتدخلات وتقديم الدعم للطلاب و/أو الموظفين بما يتماشى مع السياسة ذات الصلة (على سبيل المثال، سياسة التوظيف في دائرة التعليم والمعرفة، سياسة رفاهية الموظفين، سياسة الشؤون الإدارية للطلاب في دائرة التعليم والمعرفة، سياسة مشاركة أولياء الأمور في دائرة التعليم والمعرفة ، سلوك الطلاب في دائرة التعليم والمعرفة السياسة، وسياسة حماية الطلاب الخاصة بدائرة التعليم والمعرفة). عند الاقتضاء، يجب على المدارس الإبلاغ عن الحوادث الرقمية إلى دائرة التعليم والمعرفة والتعاون مع شرطة أبوظبي لإجراء التحقيقات.

.3يجب على المدارس التأكد من تسجيل كل حادث رقمي وتوثيقه وتوقيعه من قبل مدير المدرسة وتخزينه لأغراض التدقيق، بما يتماشى مع سياسة السجلات الخاصة بدائرة التعليم والمعرفة.

4.4يجب على المدارس أن تطلب من أولياء الأمور مراقبة استخدام الطلاب للأجهزة الرقمية خارج مباني المدرسة وساعات الدراسة لضمان السلوك الرقمي الآمن والمناسب.

5.البنية التحتية الرقمية

5.1الأجهزة الرقمية: يجب على المدارس التأكد من أن الأجهزة الرقمية الصادرة لأعضاء
يتمتع المجتمع المدرسي بميزات أمان مناسبة. عندما تسمح المدرسة للموظفين بالوصول إلى البيانات أو الأنظمة المتعلقة بالمدرسة على أجهزة أخرى أو لديها
سياسة إحضار جهازك الخاص (BYOD)للموظفين أو الطلاب، يجب على المدرسة تحديد وتنفيذ احتياطات السلامة الرقمية (على سبيل المثال، الحد الأدنى من
مواصفات الجهاز ومكافحة الفيروسات متطلبات).

5.2الأنظمة الرقمية للموظفين: يجب على المدارس التأكد من أن الموظفين المعنيين لديهم هذه الأنظمة
الوصول إلى الأنظمة الرقمية التي تقدمها دائرة التعليم والمعرفة، بما في ذلك نظام إدارة التعلم.

5.3الاستعداد للتعلم عن بعد: يجب على المدارس اعتماد تدابير للتعلم عن بعد في حالات الطوارئ مثل إغلاق المدارس مؤقتًا أو للطلاب الفرديين في ظروف استثنائية
(على سبيل المثال، الإقامة الطويلة في المستشفى، أو السفر الطارئ مع أولياء الأمور لفترات طويلة).

5.4التكنولوجيا المساعدة: يجب على المدارس توفير التكنولوجيا المساعدة للطلاب
احتياجات التعلم الإضافية كما هو موضح في خطة التعلم الموثقة، بما يتماشى مع سياسة الدمج الخاصة بدائرة التعليم والمعرفة.

5.5مقدمو الخدمات والمنتجات الخارجية:

.1يجب على المدارس تطوير إطار عمل لتقييم المخاطر بواسطة طرف ثالث لاختيار موفري خدمات تكنولوجيا المعلومات الخارجيين والمنتجات ذات الصلة بشبكة المدرسة ونظامها
وبنيتها التحتية، بما في ذلك موفري تطبيقات التعلم والتطبيقات مفتوحة المصدر. ويجب أن يتضمن هذا الإطار ما يلي كحد أدنى: أ. التوافق مع الأنظمة المدرسية الحالية.

ب. الإدارة الآمنة للبيانات.
ج. الامتثال لمعايير وأطر الأمن السيبراني.
د. الأمن ضد التهديدات السيبرانية. ه. تقديم الخدمات وأحكام النسخ الاحتياطي/الاسترداد.

F.السمعة والاستقرار المالي للمزود. ز. التزام البائع بالمرسوم بقانون اتحادي رقم (45)لسنة 2021في شأن حماية البيانات الشخصية وشروط
وأحكام دائرة التعليم والمعرفة، وسياسة حقوق النشر، وسياسة خصوصية البيانات فيما يتعلق بجمع المعلومات واستخدامها والإفصاح عنها.

ح. حيثما كان ذلك مناسبًا (على سبيل المثال، مقدمو تطبيقات التعلم)، جودة التعليم،
وملاءمة المحتوى للعمر.

.2يجب على المدارس إبلاغ الموردين الخارجيين بأن البائع خاضع للمرسوم بقانون اتحادي رقم (45)لسنة 2021في شأن حماية البيانات الشخصية

وشروط وأحكام دائرة التعليم والمعرفة، وسياسة حقوق النشر، وسياسة خصوصية البيانات فيما يتعلق بجمع المعلومات واستخدامها والكشف عنها.

6.البيانات والأمن السيبراني

6.1هندسة تكنولوجيا المعلومات الرقمية الآمنة: يجب على المدارس إنشاء بيئة رقمية آمنة وقوية
البنية التحتية والتأكد من تنفيذ ضوابط الأمن السيبراني ذات الصلة على النحو التالي:

.1التحكم في الوصول

أ. تنفيذ آليات المصادقة متعددة العوامل عبر الحرجة

خدمات.

ب. تحديد وإنفاذ التحكم في الوصول على أساس الدور لضمان حصول المستخدمين على ذلك

الأذونات المناسبة.

.2تشفير البيانات أ. استخدم التشفير للبيانات أثناء النقل والباقي لحماية البيانات الحساسة

معلومة.

.3أمن الشبكات أ. نشر جدران الحماية من الجيل التالي وأنظمة كشف/منع التسلل للحماية من الوصول غير المصرح به.

ب. تأكد من تطبيق سياسات تصفية الويب. ج. التأكد من القدرة على حظر المحتوى غير المناسب. د. القدرة على اكتشاف الأجهزة المصابة عبر شبكة المدرسة. ه. تأكد من تنفيذ جدران الحماية القائمة على الهوية لتوفير التفاصيل

الرؤية على نشاط تصفح المستخدم. .Fإنشاء بنية حافة أمنية موحدة لجميع تصفح الإنترنت. ز. مراقبة وتدقيق حركة مرور الشبكة بشكل منتظم بحثًا عن الأنماط غير المعتادة.

.4حماية نقطة النهاية

أ. تثبيت وتحديث برامج مكافحة الفيروسات/البرامج الضارة على جميع الأجهزة التي تديرها المدرسة. ب. تنفيذ تشفير جهاز القرص الصلب وضمان الأمان المنتظم

الترقيع.

.5النسخ الاحتياطي للبيانات واستعادتها

أ. إنشاء إجراءات النسخ الاحتياطي المنتظمة الآلية للبيانات الهامة. ب. تأكد من تخزين النسخ الاحتياطية وتخزينها في وضع عدم الاتصال. ج. قم بتطوير خطة قوية للتعافي من الكوارث لتقليل وقت التوقف عن العمل في حالة وقوع حادث أمني.

.6أمن البيانات أ. إنشاء ضوابط لتصنيف البيانات عبر بيانات المدرسة والطلاب. ب. قم بتنفيذ أدوات منع فقدان البيانات لضمان منع تسرب البيانات أو تسربها.

.7التدريب على التوعية الأمنية

أ. إجراء دورات تدريبية منتظمة للموظفين والطلاب لرفع مستوى الوعي حول تهديدات الأمن السيبراني وأفضل الممارسات.

.8خطة الاستجابة للحوادث

أ. تطوير وتحديث خطة الاستجابة للحوادث بانتظام لمعالجة الخروقات الأمنية بسرعة وفعالية. ب. قم بإجراء محاكاة للهجوم الإلكتروني على الطاولة وقم بالتمرين بمشاركة إدارة المدرسة.

.9الأمن الجسدي أ. ضمان الوصول الآمن إلى الخوادم الفعلية ومعدات الشبكات والبنية التحتية الحيوية الأخرى.

10. الامتثال التنظيمي
أ. ضمان الامتثال للوائح والمعايير المحلية والدولية لحماية البيانات.

11. الرصد والتسجيل
أ. تنفيذ أنظمة مراقبة شاملة للكشف عن الحوادث الأمنية والاستجابة لها في الوقت الفعلي.

ب. الاحتفاظ بسجلات مفصلة لأغراض التدقيق والتحليل.

12. تطوير البرمجيات الآمنة
أ. اتبع ممارسات الترميز الآمنة عند التطوير أو الشراء
البرامج التعليمية.
ب. قم بتحديث البرامج وتصحيحها بانتظام لمعالجة نقاط الضعف.

13. الأمن السحابي
أ. في حالة استخدام الخدمات السحابية، تأكد من التزام مقدمي الخدمات المختارين بمعايير الأمان الصارمة.

ب. تنفيذ التكوين المناسب وضوابط الوصول للموارد السحابية.
ج. دمج الخدمات السحابية – البرامج كخدمة (SaaS) مع المدرسة
خدمات الهوية حيثما أمكن ذلك.
د. إنشاء إمكانات إدارة الوضع الأمني للسحابة SaaS.

14. أمن التعاون
أ. تأمين منصات الاتصال والتعاون لحماية المعلومات التعليمية الحساسة المشتركة بين الطلاب والموظفين.

15. أمن الطرف الثالث
أ. فحص ومراقبة البائعين الخارجيين الذين يقدمون التكنولوجيا التعليمية
حلول للتأكد من أنها تلبي معايير الأمان.

6.2 صيانة النظام: يجب على المدارس صيانة النظام الرقمي وتحديثه بانتظام
البنية التحتية وأنظمة التشغيل وأنظمة الأمان والبرمجيات، بما في ذلك برامج الحماية من الفيروسات. يجب على المدارس اختبار بنيتها التحتية وأنظمتها
الرقمية بانتظام للتأكد من أنها في حالة عمل جيدة.

6.3 الاستخدام الآمن لتطبيقات التعلم الخارجي: يجب أن تتمتع المدارس بالحماية
الآليات المعمول بها (على سبيل المثال، أنظمة تسجيل الدخول الموحد) لحماية أمن الطلاب والنظام عند استخدام تطبيقات التعلم الخارجية.

6.4 التفاعل الافتراضي الآمن مع الزوار المدعوين: يجب على المدارس الحصول على موافقة أولياء الأمور على أي تفاعلات افتراضية مباشرة مع الزوار المدعوين، داخل الفصل أو خارجه. يجب أيضًا أن تتم الموافقة على جميع هذه التفاعلات من قبل دائرة التعليم والمعرفة، بما يتماشى مع سياسة الأنشطة والفعاليات اللامنهجية الخاصة بدائرة التعليم والمعرفة وسياسة حماية الطلاب الخاصة بدائرة التعليم والمعرفة.

6.5 النسخ الاحتياطي والتخزين: يجب على المدارس التي لديها أنظمة تخزين بيانات في الموقع التأكد من إجراء النسخ الاحتياطية للمعلومات والبرامج وإعدادات التكوين المهمة بتكرار مناسب والاحتفاظ بها لفترة زمنية مناسبة للسماح باستمرارية العمل.

1. يجب على المدارس التأكد من تخزين هذه النسخ الاحتياطية بشكل آمن ومنفصل
من شبكة المدرسة .

2. يجب على المدارس التي تستخدم أنظمة سحابية خارجية للتخزين التأكد من أنها
تتم مزامنة البيانات مع السحابة.

6.6حوادث الأمن السيبراني: يجب على المدارس تطوير الاستجابة واستمرارية الأعمال
خطط لتوجيه الموظفين في حالة وقوع حادث يتعلق بالأمن السيبراني، بما في ذلك بروتوكولات الإبلاغ عن الحادث إلى فريق قيادة المدرسة وإلى دائرة التعليم والمعرفة، وعملية الحفاظ على استمرارية العمليات.

.1لا يجوز للمدارس إبلاغ أي حادث يتعلق بالأمن السيبراني إلى أطراف خارجية باستثناء مقدم الخدمة المعني ودائرة التعليم والمعرفة.

.2يجب على المدارس الالتزام بجميع القوانين والسياسات المعمول بها والتي حددتها هيئة أبوظبي الرقمية وأي سلطات أخرى معنية في دولة الإمارات العربية المتحدة، بما في ذلك المرسوم بقانون اتحادي رقم (34)لسنة 2021في شأن مكافحة الشائعات والجرائم الإلكترونية.

.7حماية البيانات

7.1سياسة حماية البيانات: يجب على المدارس وضع سياسة لحماية البيانات، تحدد كيفية ضمان المدرسة للتعامل مع المعلومات الشخصية بشكل صحيح وآمن، وبما يتوافق مع المرسوم بقانون اتحادي رقم (45)لسنة 2021بشأن حماية البيانات الشخصية والتي يجب أن تشمل كحد أدنى:

.1تحديد أنواع المعلومات الشخصية التي يمكن جمعها.

.2متطلبات وإجراءات الموافقة الفردية في التحصيل،
معالجة وتخزين المعلومات الشخصية.
أ. ويجب أن تكون الموافقة حرة ومحددة ومستنيرة ولا لبس فيها.
ب. ويجوز للفرد سحب الموافقة في أي وقت.

.3الشروط التي بموجبها يجوز للمدرسة مشاركة المعلومات الشخصية مع أفراد أو كيانات أخرى (على سبيل المثال، مع دائرة التعليم والمعرفة). أ. يجب أن يكون لدى المدارس اتفاقية عدم إفشاء مدمجة في أي اتفاقيات

مع المقاولين الذين لا يمكن مشاركة بياناتهم الشخصية داخل الدولة أو خارجها لأي غرض، دون الحصول على موافقة صريحة من دائرة التعليم والمعرفة.

7.2مشاركة البيانات مع دائرة التعليم والمعرفة: يجب على المدارس توفير بيانات دقيقة وحديثة لهم
تفويض موظفي دائرة التعليم والمعرفة عند الطلب، تماشياً مع المرسوم بقانون اتحادي رقم (18)لسنة 2020في شأن التعليم الخاص والقانون رقم (9)لسنة 2018في شأن إنشاء دائرة التعليم والمعرفة وتماشياً مع شروط دائرة التعليم والمعرفة الشروط وسياسة خصوصية البيانات فيما يتعلق بجمع المعلومات واستخدامها والكشف عنها.

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

7.3خطة حماية البيانات: يجب على المدارس تطوير ومراجعة خطة حماية البيانات سنويًا، بما يتوافق مع المرسوم بقانون اتحادي رقم (45)لسنة 2021بشأن حماية البيانات الشخصية وسياسة سجلات دائرة التعليم والمعرفة. يجب أن تحدد خطة حماية البيانات الخطوات التي اتخذتها المدرسة لحماية بياناتها التنظيمية، بما في ذلك طرق تصنيف البيانات، ومستويات الترخيص، والحماية من الأمن السيبراني والتهديدات الأخرى، وإجراءات استعادة المعلومات الاحتياطية في حالة حدوث انتهاكات.

8.الاتصالات الرقمية

8.1سياسة الوسائط الرقمية: يجب على المدارس تطوير الوسائط الرقمية وتنفيذها ومراقبتها
السياسة التي تحكم إنشاء ونشر الوسائط الرقمية. ويجب أن تتضمن السياسة كحد أدنى ما يلي:

.1شرط الحصول على الموافقة قبل التسجيل والنشر الرقمي
وسائط:
أ. يجب على المدارس التقاط صور و/أو تسجيلات فيديو للطلاب فقط بعد الحصول على موافقة كتابية من أولياء الأمور. عند الحصول على الموافقة، يجب على المدارس إبلاغ أولياء الأمور بالأغراض التي يتم من أجلها التقاط الصور و/أو تسجيلات الفيديو.

ب. يجب على المدارس الحصول على موافقة كتابية من أولياء الأمور قبل نشر المحتوى الرقمي الذي يشمل الطلاب. يجب على المدارس أن تحدد بوضوح ما إذا كان سيتم تعريف الطالب بالاسم في المنشور عند الحصول على الموافقة.

.2إجراءات تقديم الموافقة وسحبها.

.3الشروط المتعلقة بتخزين وأمن الوسائط الرقمية.

.4الشروط المتعلقة باستخدام الأجهزة والحسابات الشخصية للتسجيل
أو نشر المحتوى المدرسي.

8.2سياسة وسائل التواصل الاجتماعي: يجب على المدارس تطوير وتنفيذ سياسة وسائل التواصل الاجتماعي في
-علاقة استخدام المدرسة لوسائل التواصل الاجتماعي.

.1يجب أن تتضمن السياسة كحد أدنى ما يلي:
أ. منصات وحسابات التواصل الاجتماعي التي ستستخدمها المدرسة.
ب. إجراءات الوصول والأمن وحماية كلمة المرور الخاصة بالمدرسة
حسابات وسائل التواصل الاجتماعي.
ج. الشروط المتعلقة بالمحتوى واستخدام اللغة والتفاعل مع الآخرين
حسابات.
د. الشروط المتعلقة باستخدام الأسماء والصور ومقاطع الفيديو للطلاب،
وفقًا للقسم .8.1سياسة الوسائط الرقمية.
ه. إرشادات للمشرفين (انظر القسم .8.2.2المشرفون) فيما يتعلق بالمحتوى الذي تنشره أطراف ثالثة على صفحات وسائل التواصل الاجتماعي الخاصة بالمدرسة، بما في ذلك إجراءات إدارة المحتوى غير المحترم والتصيد.

F.إجراءات معالجة السلوكيات السلبية الأخرى على وسائل التواصل الاجتماعي، مثل
انتحال حسابات المدرسة.

.2مراقبة الاتصالات المدرسية: يجب على المدارس مراقبة جميع قنوات الاتصال الرسمية وغير الرسمية ذات الصلة بالمدرسة (النشرات الإخبارية، ووسائل التواصل الاجتماعي، ومجموعات التواصل مع أولياء الأمور، وما إلى ذلك) بانتظام لضمان امتثالها لهذه السياسة.

.3المشرفون: يجب على المدارس تعيين مشرف (وسطاء) للموافقة المسبقة على المحتوى الذي ينشره المستخدمون الآخرون على صفحات وسائل التواصل الاجتماعي الخاصة بالمدارس أو إزالته، حيثما أمكن ذلك، بما يتماشى مع إرشادات المدرسة. يجب على المشرف (المشرفين) رفض أو إزالة، حيثما أمكن ذلك، المحتوى غير المناسب، الذي لا يتماشى مع القيم الثقافية لدولة الإمارات العربية المتحدة، أو الذي يرقى إلى مستوى التنمر أو المضايقة أو التمييز أو الترهيب، بما يتماشى مع سياسة القيم والأخلاقيات لدائرة التعليم والمعرفة ودائرة التعليم والمعرفة . سياسة الاعتبارات الثقافية.

8.3حسابات وسائل التواصل الاجتماعي الشخصية للموظفين: يجب على المدارس السماح لأعضاء هيئة التدريس بإنشاء حسابات شخصية موجودة على وسائل التواصل الاجتماعي والحفاظ عليها. وفيما يتعلق بهذه الأمور، يجب على الموظفين ما يلي:

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

.2استخدم أضيق إعدادات الخصوصية الممكنة.

.3عدم تعريف أنفسهم بأنهم مرتبطين بالمدرسة إلا على
منصات التواصل الاجتماعي الاحترافية (مثل .LinkedIn)

.4عدم قبول دعوات الصداقة أو التواصل مع أو متابعة الطلاب الحاليين أو الطلاب السابقين الذين تقل أعمارهم عن 18عامًا، أو إرسال مثل هذه الطلبات للطلاب الحاليين أو الطلاب السابقين الذين تقل أعمارهم عن 18عامًا.

.5عدم قبول الدعوات من أولياء أمور الطلاب الحاليين للتعارف والتواصل
معهم أو متابعتهم.

.6عدم استخدام مثل هذه الحسابات للتواصل مع الطلاب الحاليين أو أولياء أمورهم أو الطلاب السابقين الذين تقل أعمارهم عن 18عامًا. وينطبق ذلك على تطبيقات المراسلة (مثل .WhatsApp، Telegram، Signal)

.7افترض أن المحتوى المنشور من خلال هذه الحسابات (بما في ذلك المراجعات والتعليقات عبر الإنترنت) مرئي للعامة وقابل للبحث، بغض النظر عن إعدادات الخصوصية، ومارس التقدير المناسب.

.8التأكد من أن المحتوى الذي تتم مشاركته من خلال هذه الحسابات مناسب، بما يتماشى مع سياسة الاعتبارات الثقافية لدائرة التعليم والمعرفة، ولا يرقى إلى مستوى التنمر أو المضايقة أو التمييز أو الترهيب، بما يتماشى مع سياسة القيم والأخلاقيات الخاصة بدائرة التعليم والمعرفة.

.9التأكد من أن المحتوى الذي تتم مشاركته من خلال هذه الحسابات لا يعطي انطباعًا بتأييد المدرسة.

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

8.4الاتصالات عبر البريد الإلكتروني: يجب على المدارس إبلاغ أعضاء هيئة التدريس بأنه غير مصرح لهم باستخدام عناوين البريد الإلكتروني الشخصية للتواصل مع الطلاب أو أولياء الأمور.

8.5موقع المدرسة: يجب على المدارس إنشاء موقع ويب مخصص وتحديثه باستمرار
-أن تكون مرجعاً لأعضاء المجتمع المدرسي.

.1يجب على المدارس نشر المحتوى التالي على موقعها الإلكتروني كحد أدنى:
أ. معلومات الاتصال.
ب. الخدمات التي تقدمها المدرسة.
ج. الرسوم، بما في ذلك رسوم النقل ورسوم الأنشطة الاختيارية.
د. تقارير التفتيش.
ه. بيانات تحصيل الطلاب الإجمالية أو الإنجازات الفردية (على سبيل المثال،
الجوائز) بموافقة.
.Fالإصدارات العامة من التقرير السنوي، بما يتماشى مع تقارير دائرة التعليم والمعرفة
سياسة.

ز. سياسات المدرسة ذات الصلة بأولياء الأمور و/أو الطلاب.
ح. أي محتوى آخر مطلوب، على النحو المحدد في سياسات دائرة التعليم والمعرفة.

.2يجب على المدارس التأكد من أن المحتوى المنشور على موقعها الإلكتروني دقيق ومناسب، بما يتماشى مع سياسة القيم والأخلاقيات الخاصة بدائرة التعليم والمعرفة.

.3يجب على المدارس التأكد من أن المحتوى المنشور على موقعها الإلكتروني يتماشى مع متطلبات الوسائط الرقمية (انظر القسم .9.1سياسة الوسائط الرقمية).

.9الامتثال

9.1تسري هذه السياسة اعتبارًا من بداية العام الدراسي 2024/25(فصل الخريف).
ومن المتوقع أن تلتزم المدارس بهذه السياسة بشكل كامل مع بداية العام الدراسي 2025/26(فصل الخريف).

9.2يخضع عدم الالتزام بهذه السياسة للمساءلة القانونية والعقوبات المنصوص عليها وفقًا لأنظمة وسياسات ومتطلبات دائرة التعليم والمعرفة، بغض النظر عن أي عقوبات أخرى يفرضها المرسوم بقانون اتحادي رقم (31)لسنة 2021بإصدار الجرائم والعقوبات القانون أو أي قانون آخر ذي صلة. تحتفظ دائرة التعليم والمعرفة بالحق في التدخل إذا تبين أن المدرسة تنتهك التزاماتها.

مراجع

•دائرة التعليم والمعرفة في أبوظبي .(ADEK)(اختصار الثاني). شروط الاستخدام وبيان الخصوصية للمعلومات. •جمعية صناعة التكنولوجيا المساعدة .(ATIA)(اختصار الثاني). ما هو في؟

•مرسوم بقانون اتحادي رقم (3)لسنة 2016في شأن حقوق الطفل.
•مرسوم بقانون اتحادي رقم (18)لسنة 2020في شأن التعليم الخاص.
•مرسوم بقانون اتحادي رقم (31)لسنة 2021بإصدار قانون الجرائم والعقوبات.
•مرسوم بقانون اتحادي رقم (34)لسنة 2021في شأن مكافحة الشائعات والجرائم الإلكترونية.
•مرسوم بقانون اتحادي رقم (38)لسنة 2021في شأن حقوق المؤلف والحقوق المجاورة.
•مرسوم بقانون اتحادي رقم (45)لسنة 2021في شأن حماية البيانات الشخصية.
•آي بي إم. (اختصار الثاني). ما هي الاستجابة للحوادث؟
•قانون رقم (9)لسنة 2018في شأن إنشاء دائرة التربية والتعليم

معرفة.

•وزارة التربية والتعليم. .(2022)قواعد السلوك للمهنيين بشكل عام

تعليم.

•وزارة التربية والتعليم. (اختصار الثاني). السياسة الوطنية للوقاية من التنمر في المؤسسات التعليمية.

•رابطة صناعة شبكات التخزين .(SNIA)(اختصار الثاني). ما هي حماية البيانات؟
•المجلس الأعلى لمركز مراقبة ومراقبة الأمن الوطني .(2022) .(MCC)

دليل أجهزة المراقبة (الطبعة الأولى. .(V1.0.2022

•جامعة تافتس. (اختصار الثاني). نظرة عامة على وسائل التواصل الاجتماعي.

النشر

0.1.v_السياسة الرقمية_loohcS_KEDA (يناير)2024

دائرة المعرفة والتعليم (ADEK)

تحل هذه السياسة محل السياسة 13(الموقع الإلكتروني) والسياسة 65(الحماية من مخاطر شبكة المعلومات العالمية (الإنترنت)) في دليل سياسات وإرشادات المدارس الخاصة 2014-2015.

تنطبق هذه السياسة على المدارس المستقلة. ومع ذلك، فإن أي تعميم صادر قبل هذه السياسة أو تم إصداره خصيصًا للمدارس المستقلة بعد ذلك يحل محل متطلبات هذه السياسة.