سياسة الذكاء الاصطناعي والتكنولوجيا

المواءمة مع إطار تفتيش المدارس في دولة الإمارات العربية المتحدة

تتماشى هذه السياسة مع معيار تفتيش المدارس في دولة الإمارات العربية المتحدة 4.1 تصميم المنهج وتنفيذه :العنصران 4.1.1 الأساس المنطقي والتوازن والامتثال و 4.1.4 .الروابط عبر المناهج، ومعيار 5.1 الصحة والسلامة، بما في ذلك ترتيبات حماية الطفل/الصون :العنصر 5.1.2 الترتيبات اللازمة لضمان الصحة والسلامة والأمن

السياسة

1. الذكاء الاصطناعي ومحو الأمية الرقمية

1.1 **دمج المنهج** :يجب على المدارس تطوير محو أمية الطلاب في الذكاء الاصطناعي والرقمية من خلال منهجها مع تزايد التعقيد التقني، بما يتماشى مع **الملحق أ** .متطلبات محو الأمية في الذكاء الاصطناعي

1.2**رصد مخرجات تعلم الذكاء الاصطناعي والإبلاغ عنها** :يجب على المدارس اعتماد نظام إدارة يدمج معايير الذكاء الاصطناعي ومخرجات التعلم lms بما .يضمن أن تكون بيانات محو أمية الطلاب في الذكاء الاصطناعي متاحة لدائرة التعليم والمعرفة لأغراض الرصد التنظيمي.

1.3 **تقييم محو الأمية في الذكاء الاصطناعي** :يجب على المدارس ضمان تخرج كل طالب مع إظهار محو الأمية في الذكاء الاصطناعي، ويتم تقييم ذلك من خلال .تطبيق الطلاب للمعرفة والمهارات في سياقات أصيلة وواقعية، وتكييفه للطلاب ذوي احتياجات التعلم الإضافية، بما يتماشى مع سياسة الدمج

2. أدوات تعلم الذكاء الاصطناعي

2.1 التعلم الشخصي المدعوم بالذكاء الاصطناعي :يجب على المدارس تنفيذ واحدة على الأقل من أدوات التعلم الشخصي المدعومة بالذكاء الاصطناعي. أدوات تعلم الذكاء الاصطناعي "بما في ذلك معلمو الذكاء الاصطناعي القائمون على المحادثة أو غير القائمين على المحادثة (التي تستوفي متطلبات **الملحق ب.** معايير أداة تعلم الذكاء الاصطناعي، والحصول على موافقة دائرة التعليم والمعرفة قبل نشر أي أداة من خلال إكمال "نموذج تدقيق أداة تعلم الذكاء الاصطناعي الخاص بدائرة التعليم والمعرفة ."يجب على المدارس وضع حدود لوقت الشاشةالاعلى للتعلم.

2.2 الكفاءة التأسيسية "الذكاء الاصطناعي للتدريس:" يجب على المدارس ضمان إكمال جميع موظفي التدريس والدعم التعليمي المعنيين تدريباً تأسيسياً على استخدام أدوات تعلم الذكاء الاصطناعي لتحديد نقاط القوة والضعف لدى الطلاب وتكييف طرق التدريس لمعالجة فجوات التعلم، بما يتماشى مع **الملحق ج.** المتطلبات التربوية .لاستخدام أدوات تعلم الذكاء الاصطناعي

2.3 ،تدريب الطلاب على أداة تعلم الذكاء الاصطناعي: يجب على المدارس تدريب جميع الطلاب على استخدام أدوات تعلم الذكاء الاصطناعي المنشورة لديها بما يضمن قدرة الطلاب على التنقل في الأداة، واستخدام الأداة لدعم تعلمهم الذاتي، وصياغة الموجهات)إن انطبق(، والالتزام بحواجز السلامة، والانخراط في الاستخدام .المسؤول.

3.الجاهزية المؤسسية

3.1 الاستراتيجية الرقمية: تطوير وتنفيذ استراتيجية رقمية سنوية على مستوى المدرسة لاستخدام الذكاء الاصطناعي والتكنولوجيا لتحسين تحصيل الطلاب، والتربية .التعليمية، وعمليات المدرسة

3.2 التطوير المهني المستمر في الذكاء الاصطناعي :يجب على المدارس ضمان حضور الموظفين لجميع التدريبات التي تفرضها دائرة التعليم والمعرفة)العامة والمحددة حسب الدور، عندما ينطبق ذلك .(يجب توفير فرص التطوير المهني المستمر للموظفين في استخدام الذكاء الاصطناعي المتمحور حول الإنسان، والممارسات الأخلاقية والمسؤولة للذكاء الاصطناعي، وأنظمة وتطبيقات الذكاء الاصطناعي، والتربية التعليمية المدعومة بالذكاء الاصطناعي، والذكاء الاصطناعي للنمو والتحسين المهني، والأمن السيبراني .والسلامة الرقمية.

3.3 البنية التحتية والأنظمة الرقمية :يجب على المدارس الحفاظ على بنية تحتية وأنظمة رقمية موثوقة(مثل الشبكات، والتطبيقات، والأجهزة، والخدمات) بما يتماشى مع ، **الملحق د.** المتطلبات الفنية، بما في ذلك على سبيل المثال لا الحصر الأجهزة الآمنة الصادرة عن المدرسة وتدابير السلامة لترتيبات إحضار جهازك الخاص ، ووصول الموظفين إلى الأنظمة والمنصات الرقمية التي توفرها دائرة التعليم والمعرفة، والجاهزية للتعلم عن بعد المعتمد من دائرة التعليم والمعرفة، وأي تقنيات مساعدة، بما يتماشى مع سياسة الدمج .

الاستخدام المسؤول .4

4.1 سياسات الاستخدام المسؤول: يجب على المدارس تنظيم الاستخدام المسؤول للذكاء الاصطناعي والتكنولوجيا لحماية التعلمباعلى درجة وضمان السلوك الأكاديمي ،

4.2 استخدام الطلاب للهاتف :لا يجوز السماح للطلاب باستخدام الهواتف المحمولة الشخصية داخل مباني المدرسة خلال اليوم الدراسي(ما لم يصرح المعلم بذلك صراحة وبصورة استثنائية لأغراض التعلم .(يجب على المدارس ضمان تعطيل الاتصال في الأجهزة الأخرى المزودة ببطاقات مثل الساعات الذكية، وأن الأجهزة اللازمة للتعلم مثل الأجهزة اللوحية والحواسيب المحمولة .تستخدم فقط لأغراض التعلم وتراقب بفعالية لمنع التشتت.

4.3 استخدام الطلاب لوسائل التواصل الاجتماعي :لا يجوز للمدارس السماح للطلاب باستخدام وسائل التواصل الاجتماعي، بما يتماشى مع قرار مجلس الوزراء رقم 106 لسنة .بشأن تنظيم وصول الأطفال إلى وسائل التواصل الاجتماعي وتعديلاته 2026

4.4 لا يجوز للمدارس السماح باستخدام الشبكات الخاصة الافتراضية VPNاستخدام الشبكات الخاصة الافتراضية VPN على أي جهاز داخل مباني المدرسة وشبكاته

4.5 الشراكة مع أولياء الأمور: يجب على المدارس إبلاغ أولياء الأمور بانتظام بالتزامهم بمراقبة السلوك الرقمي لأطفالهم خارج المدرسة والحد من استخدام وسائل التواصل الاجتماعي للأطفال الذين تبلغ أعمارهم 15 عاماً فأقل، بما يتماشى مع المرسوم بقانون اتحادي رقم 26 لسنة 2025 بشأن السلامة الرقمية للطفل وقرار مجلس الوزراء رقم .لسنة 2026 بشأن تنظيم وصول الأطفال إلى وسائل التواصل الاجتماعي وتعديلاتهما (106)

5. الأمن

5.1 اختيار الموردين :يجب على المدارس وضع إجراءات لاختيار وإدارة موردي التكنولوجيا الخارجيين والمنتجات والخدمات التي تستوفي متطلبات دائرة التعليم والمعرفة وقوانين دولة الإمارات العربية المتحدة.

5.2 الحوادث الرقمية، :يجب على المدارس تحديد الحوادث الرقمية وإدارتها وتوثيقها والاستجابة لها والإبلاغ عنها، مع دعم الطلاب المتأثرين وإبلاغ أولياء الأمور حسب الاقتضاء بما يتماشى مع سياسة حماية الطالب، وسياسة سلوك الطالب، وسياسة السجلات، وقوانين دولة الإمارات العربية المتحدة المعمول بها.

5.3 حماية البيانات والأمن السيبراني :يجب على المدارس تنفيذ وصيانة تدابير حماية البيانات والأمن السيبراني، بما يتماشى مع **الملحق د** .المتطلبات الفنية، والمرسوم بقانون اتحادي رقم 45 لسنة 2021 بشأن حماية البيانات الشخصية، والمرسوم بقانون اتحادي رقم 34 لسنة 2021 بشأن مكافحة الشائعات والجرائم الإلكترونية، والمرسوم بقانون اتحادي رقم 26 لسنة 2025 بشأن السلامة الرقمية للطفل، وتعديلاتها، وأي قوانين ومتطلبات أخرى صادرة عن الجهات الحكومية المختصة.

5.4 الاتصال الرقمي ووسائل التواصل الاجتماعي :يجب على المدارس تنفيذ التخزين الآمن والاستخدام المناسب للوسائط الرقمية، ووضع ضوابط للحسابات الرسمية للمدرسة على وسائل التواصل الاجتماعي، ومراقبة قنوات الاتصال الرسمية وغير الرسمية المتعلقة بالمدرسة، والحصول على موافقة أولياء الأمور قبل تسجيل أو نشر وسائط رقمية يمكن التعرف فيها على الطالب.

5.5 ممارسات الاتصال الشخصية للموظفين: يجب على المدارس إبلاغ الموظفين بالممارسات غير المصرح بها، بما في ذلك استخدام البريد الإلكتروني الشخصي أو حسابات وسائل التواصل الاجتماعي للتواصل مع الطلاب الحاليين، أو الطلاب السابقين الذين تقل أعمارهم عن 18 عاماً، أو أولياء الأمور، أو استخدام حسابات وسائل التواصل الاجتماعي الشخصية لنشر معلومات مدرسية سرية أو محتوى قد يكون غير مناسب، أو تمييزياً، أو ضاراً، أو يُنظر إليه على أنه معتمد من المدرسة.

6. الاتصالات

6.1 الموقع الإلكتروني للمدرسة: يجب على المدارس الحفاظ على موقع إلكتروني محدث للمدرسة يحتوي على جميع المعلومات التي تفرضها دائرة التعليم والمعرفة.

الامتثال

من المتوقع أن تكون المدارس ممتثلة بالكامل لهذه السياسة بحلول العام الدراسي 2027/28(.فصل الخريف)

إن عدم الامتثال لهذه السياسة سيخضع للمساءلة القانونية والعقوبات المنصوص عليها وفقاً للوائح دائرة التعليم والمعرفة وسياساتها ومتطلباتها، دون الإخلال بأي عقوبات أخرى يفرضها المرسوم بقانون اتحادي رقم 31 (لسنة 2021 بإصدار قانون الجرائم والعقوبات وتعديلاته أو أي قانون آخر ذي صلة .تحتفظ دائرة التعليم والمعرفة بالحق في التدخل إذا تبين أن المدرسة تخالف التزاماتها.

المخرجات المتوقعة

:ستقيّم دائرة التعليم والمعرفة أثر هذه السياسة من خلال المخرجات المتوقعة الآتية

1. تحسن محو الأمية في الذكاء الاصطناعي والرقمية لدى الطلاب
2. تعزيز التربية التعليمية المدعومة بالذكاء الاصطناعي لدى المعلمين
3. تحسين مخرجات تعلم الطلاب)التحصيل والتقدم (باستخدام أدوات تعلم الذكاء الاصطناعي
4. تعزيز الاستخدام المسؤول للذكاء الاصطناعي والتكنولوجيا في المدارس

الملحق أ .متطلبات محو الأمية في الذكاء الاصطناعي

:يجب على المدارس تنفيذ إطار دائرة التعليم والمعرفة لمحو الأمية في الذكاء الاصطناعي من الروضة حتى الصف الثاني عشر على النحو الآتي

1. **دمج محو الأمية في الذكاء الاصطناعي في المنهج** :يجب على المدارس ضمان تطوير الطلاب للخيوط الأربعة المترابطة لمحو الأمية في الذكاء الاصطناعي من خلال منهجها :الفهم المفاهيمي للذكاء الاصطناعي؛ والتقييم النقدي والتفاعل المستنير؛ وإنشاء الذكاء الاصطناعي وهندسته وتصميم الأنظمة؛ والحوكمة المسؤولة وخصوصية البيانات .والأثر المجتمعي.

2. **ملفات متعلم الذكاء الاصطناعي والمراحل** :يجب على المدارس إدخال الخيوط الأربعة لمحو الأمية في الذكاء الاصطناعي عبر أربع مراحل تنموية وملفات للمتعلمين، مع التقدم بتعقيد تقني متزايد .تُعرّف الكفاءات الأساسية التي ينبغي أن يهدف الطلاب إلى تحقيقها لكل من ملفات متعلم الذكاء الاصطناعي الأربعة في الجدول 1 .ملفات ومراحل متعلم :الذكاء الاصطناعي

الجدول 1 .ملفات ومراحل متعلم الذكاء الاصطناعي

المرحلة/الحلقة	ملف متعلم الذكاء الاصطناعي	معلم الكفاءة الأساسية
:المرحلة 1/رياض الأطفال KG1-KG2/FS2-Year 1	**مستكشف واعٍ بالذكاء الاصطناعي**	يستكشف المدخلات والاستجابات من خلال اللعب يميز الطلاب بين الحواس البشرية والمدخلات الآلية الأساسية ويفهمون علاقات السبب والنتيجة يكون التعلم غير متصل .ودون استخدام مباشر لأداة الذكاء الاصطناعي
:المرحلة 2/الحلقة 1 Year 2-6/الصفوف 1-5	**مفكر ملمّ بالذكاء الاصطناعي**	.يطبق القواعد والمنطق والبيانات لتوليد المخرجات وتقييمها يتقدم الطلاب من التفكير القائم على القواعد إلى المنطق متعدد الخطوات، ويطورون فهماً لكيفية تأثير البيانات في .النتائج، ويبدؤون التفاعل مع أدوات الذكاء الاصطناعي لتحسين المخرجات
:المرحلة 3/الحلقة 2 Year 7-9/الصفوف 6-8	**باني حلول الذكاء الاصطناعي**	.يصمم ويحسن حلولاً مدعومة بالذكاء الاصطناعي باستخدام البيانات والنماذج وسير العمل .يبني الطلاب الحلول ويقيمونها ويحسنونها باستخدام عمليات منظمة ومفاهيم أساسية في تعلم الآلة
:المرحلة 4/الحلقة 3 /الصفوف 9-12 Year 10-13	**مصمم أنظمة وحلول الذكاء الاصطناعي**	.يصمم ويحكم أنظمة ذكاء اصطناعي متكاملة يطور الطلاب حلولاً واقعية باستخدام التفكير النظمي ويضمنون الفعالية والمسؤولية والاتساق مع التوقعات المجتمعية .وتوقعات الحوكمة

3. **أهداف التعلم والكفاءات** :يجب على المدارس اعتماد تصميم تعلم حلزوني لمنهج الذكاء الاصطناعي لديها، مع إعادة تناول المفاهيم التأسيسية بدرجة تعقيد متزايدة عبر الصفوف.

4. **نمط الدمج:** يجب على المدارس دمج محو الأمية في الذكاء الاصطناعي في منهجها باستخدام أحد الأنماط الآتية:

أ .**مستقل** :يُدرّس الذكاء الاصطناعي كوحدة أو مقرر مستقل واحد ضمن مادة مخصصة لتكنولوجيا المعلومات والاتصالات)مثل علوم الحاسوب، التكنولوجيا، تكنولوجيا .المعلومات والاتصالات، وما إلى ذلك (مع عدد أدنى محدد من الساعات المعتمدة كل عام لكل مرحلة

ب .مدمج :يُدمج الذكاء الاصطناعي في مواد وموضوعات متعددة، بدلاً من اقتصاره على المواد المستقلة)مثل الذكاء الاصطناعي في الرياضيات والعلوم، وما إلى ذلك(، لدعم .خبرات تعلم أصيلة وتطبيق فهم الذكاء الاصطناعي في سياقات واقعية ومتعددة التخصصات

.ج .**هجين:** يُدرّس الذكاء الاصطناعي من خلال مادة تكنولوجيا المعلومات والاتصالات المخصصة في المدرسة، وكذلك يدمج عبر مواد وموضوعات متعددة

الملحق ب .معايير أداة تعلم الذكاء الاصطناعي

يجب على المدارس تطبيق الجدول 1 .معايير أداة تعلم الذكاء الاصطناعي الإلزامية عند تقييم أدوات تعلم الذكاء الاصطناعي .يجب على المدارس التي تسعى للحصول على موافقة دائرة التعليم والمعرفة لأداة ما تقديم الأدلة مقابل كل معيار من خلال "نموذج طلب أداة تعلم الذكاء الاصطناعي الخاص بدائرة التعليم والمعرفة **."لن تُمنح الموافقة إلا للأدوات .التي تستوفي جميع المعايير الإلزامية**

الجدول 1 .معايير أداة تعلم الذكاء الاصطناعي الإلزامية

المعيار	أسئلة ومتطلبات التقييم
كشف السلامة وإيذاء النفس	1. هل تكشف الأداة عن تعبيرات إيذاء النفس، أو الأفكار الانتحارية، أو الإساءة، أو الضيق الشديد)إن انطبق(؟ 2. عند الكشف، هل تنبه المعلم و/أو مسؤول المدرسة فوراً)إن انطبق(؟ 3. هل تتيح الأداة للمعلمين تخصيص حواجز السلامة/إيذاء النفس من خلال التوجيه و/أو ميزات التهيئة؟
تصفية المحتوى الثقافي	1. هل تكشف الأداة المحتوى غير الملائم ثقافياً وتقوم بتصفيته من خلال التخصيص القائم على المحادثة أو إعدادات التهيئة؟ يشمل المحتوى غير الملائم ثقافياً: • التكاثر البشري وعقيدة التطور • الهوية الجندرية البديلة والميول الجنسية • الكحول والمخدرات • التلقين الديني/السياسي 2. هل تنبه الأداة المعلم و/أو المسؤول؟
النزاهة الأكاديمية	1. هل تكشف الأداة محاولات الانتحال وتحظرها؟
التربية التعليمية	2. هل تستخدم الأداة مناهج تربوية قائمة على الأدلة، بما في ذلك واحد أو أكثر مما يأتي: • طرح الأسئلة السقراطية)توجيه الطلاب إلى الإجابات من خلال الاستقصاء(• التعلم للإتقان)اشتراط الكفاءة قبل التقدم(• التكرار المتباعد)جدولة المراجعة على فواصل زمنية للاحتفاظ طويل الأمد(• ممارسة الاسترجاع)اختبار التذكر بدلاً من إعادة القراءة(3. هل توجه الطلاب إلى التفكير والاستدلال بدلاً من مجرد تقديم الإجابات؟
دمج المنهج والمحتوى	1. هل تدمج الأداة معايير منهج مدرستك)مثل وزارة التربية والتعليم في دولة الإمارات العربية المتحدة ، والمنهج الوطني البريطاني، ومعايير الأمريكية، والبكالوريا الدولية (IB)، وCBSE(؟ أو هل يمكن للمدرسة أو المعلم تحميل معايير/مخرجات تعلم مخصصة؟ 2. هل تربط/توسم الأداة وتبلغ عن إتقان معايير المنهج/مخرجات التعلم؟
التقييم وموارد التعلم	1. هل توفر الأداة تقييمات قبلية وبعدية تلتقط مخرجات تعلم الطلاب في بداية كل وحدة ونهايتها؟ 2. هل يمكن للمعلم استخدام الأداة لتوليد خطط دروس، وعروض تقديمية، ومجموعات تدريب، واختبارات قصيرة، ومهام متمايزة، وبنود تقييم تكويني مخصصة ومتوافقة مع معايير المنهج واحتياجات الصف)إن انطبق(؟ 3. هل يمكن للمعلم تحرير المحتوى المولد بالذكاء الاصطناعي أو تكييفه أو رفضه قبل نشره للطلاب)إن انطبق(؟
واجهة المعلم :نشاط على مستوى الطالب	1. هل يمكن للمعلم الاطلاع على كل ما يأتي لكل طالب فردي: • فجوات التعلم • مشاركة الطالب • الوقت المستغرق في الأداة • تقدم الإنجاز للمهام المسندة • معدلات إنجاز المهام المسندة • تحصيل الطالب حسب مخرج التعلم • تقدم الطالب حسب مخرج التعلم • سجل المحادثة الكامل/تاريخ المحادثة)إن انطبق(• اتجاهات الأداء عبر الزمن 2. هل تُحدد مخاوف التعلم للمعلم؟ 3. هل تنشئ الأداة تقارير تقدم مفصلة تبين اتجاهات الإتقان عبر الزمن؟
واجهة المعلم :نشاط على مستوى الصف	• هل يمكن للمعلم الاطلاع على تحليلات مستوى الصف بما في ذلك كل ما يأتي: • فجوات التعلم • مشاركة الطالب • الوقت المستغرق في الأداة • تقدم الإنجاز للمهام المسندة • معدلات إنجاز المهام المسندة • اتجاهات الأداء عبر الزمن • مقارنة أداء الطالب الفردي بخط أساس الصف
امكانية وصول المسؤول	1. هل يمكن لمسؤول المدرسة الاطلاع على: • استخدام المعلم وتفاعلاته مع الأداة • مشاركة الطالب • إكمال الطالب للمهام المسندة • سجل المحادثة الكامل)تاريخ المحادثة (للطلاب الذين تم وسمهم بسبب السلامة وإيذاء النفس وعدم الملاءمة الثقافية)إن انطبق(2. هل يمكن للمسؤول إدارة حسابات المستخدمين، والأدونات، وتهيئات الأداة على مستوى المدرسة؟ 3. هل يمكن منح دائرة التعليم والمعرفة وصولاً إدارياً على مستوى النظام لإجراء مراجعات ضمان الجودة؟

موجه الحواجز لأدوات تعلم الذكاء الاصطناعي

يجب على المعلمين نسخ/لصق أو تضمين هذا الموجه داخل واجهة أداة تعلم الذكاء الاصطناعي، بما في ذلك في تعليمات المحادثة لإنشاء الصف والمساحة، وتوليد الدروس .والواجبات، و/أو إعدادات موجه النظام لتوجيه استجابات الذكاء الاصطناعي وتقييدها قبل تفاعل الطالب

:الموجه

.أنت معلم ذكاء اصطناعي مهيأ للاستخدام في مدارس دولة الإمارات العربية المتحدة .يجب عليك الالتزام بالمعايير الثقافية والقانونية لدولة الإمارات العربية المتحدة في جميع الأوقات

:القواعد الأساسية

1. .اقصر جميع الاستجابات على موضوع الدرس المسند فقط
2. .ارفض أي أسئلة عن التكاثر البشري وعقيدة التطور، والهوية الجندرية البديلة والميول الجنسية، والكحول والمخدرات، والتلقين الديني/السياسي
3. .لا تقدم أي أرقام اتصال للدعم للطلاب في أي حالة
4. .بالنسبة لأي مخاوف تتعلق بحماية الطفل أو الصون يتم اكتشافها، شجع الطلاب على التواصل مع معلم، أو مدير، أو مرشد مدرسي، أو شخص بالغ مسؤول آخر
5. .لا تنخرط أبداً في أي شيء قد يضر بالطالب .وجّه دائماً المخاوف إلى شخص بالغ موثوق أو مرشد مدرسي
6. .شجع التواصل المحترم والإيجابي .أعد توجيه الرسائل الوقحة أو الخارجة عن الموضوع بهدوء إلى الدرس
7. .اعكس قيم دولة الإمارات في كل استجابة .تجنب أي شيء يتعارض مع القيم الإسلامية أو أعراف دولة الإمارات .لا تنتقد أبداً أي دين أو ثقافة أو جنسية
8. .عندما يُطرح الطعام، عزز الأكل الصحي والمتوازن .لا تشر أبداً إلى أطعمة محظورة بموجب الإرشادات الغذائية الإسلامية .ادعم الصورة الجسدية الإيجابية

الملحق ج .المتطلبات التربوية لاستخدام أدوات تعلم الذكاء الاصطناعي

:يجب على المعلمين ومساعدي المعلمين الذين يستخدمون أدوات تعلم الذكاء الاصطناعي استيفاء المتطلبات الآتية

:مواءمة المنهج

1. ضمان وجود حواجز للسلامة والملاءمة الثقافية من أجل السلامة، وإيذاء النفس، والملاءمة الثقافية باستخدام الموجه المبين في موجه الحواجز لأدوات تعلم الذكاء الاصطناعي)الملحق ب(.
2. .إسناد مهام تعلم مناسبة للعمر ومتماشية مباشرة مع معايير المنهج/مخرجات التعلم
3. .تكييف المهام حسب مستوى القدرة لضمان حصول جميع الطلاب، بمن فيهم ذوو احتياجات التعلم الإضافية، على مهام مناسبة لمستوى مهاراتهم

:توليد المحتوى والدروس

1. .توليد خطط الدروس، والعروض التقديمية، ومجموعات التدريب، ومواد التعلم المتمايزة باستخدام أدوات تعلم الذكاء الاصطناعي
2. .التحقق من الدقة الواقعية وضمان مواءمة المنهج لخطط الدروس والموارد المولدة بالذكاء الاصطناعي

:رصد تعلم الطلاب

1. :فحص ورصد الأداء على مستوى الطالب والصف باستخدام أداة تعلم الذكاء الاصطناعي لتحديد فجوات التعلم وإدخال التدخلات حسب الحاجة
   a. إذا كان غالبية الطلاب يظهرون فجوات تعلم في مفهوم محدد)مثل حساب المساحات تحت المنحنيات، أو فهم كيفية عمل الإنزيمات، أو الكتابة باستخدام المبني للمعلوم(، فقم بتغطية هذه المفاهيم بمزيد من التفصيل خلال الدروس المتزامنة اللاحقة لسد الفجوة على مستوى الصف)المستوى 1(.
   b. إذا كان طالب واحد فقط أو عدد قليل من الطلاب يواجهون صعوبات، يجب على المعلمين تقديم تدخلات أكثر استهدافاً على مستوى 1:1 أو المجموعات الصغيرة)المستوى 2 أو 3 (حسب المطلوب)مثل جلسات موجزة مدتها 5 دقائق من خلال ساعات مكتبية فردية، أو جلسة فرعية متزامنة مدتها 5-10 دقائق للمجموعة المستهدفة أو الفرد بينما يعمل باقي الصف على عمل غير متزامن(.
2. .إعادة تهيئة أداة تعلم الذكاء الاصطناعي لاختبار ما إذا كان الطلاب قد فهموا المفاهيم وللتحقق مما إذا كان التدخل فعالاً في سد فجوات التعلم
3. مراجعة بيانات مستوى الطالب على أدوات تعلم الذكاء الاصطناعي أسبوعياً لضمان مشاركة الطالب وإكمال الواجبات، مع مراقبة المحتوى غير الملائم الخارج عن الموضوع على أداة تعلم الذكاء الاصطناعي.
4. .مراجعة بيانات الطلاب الإجمالية على مستوى الصف على أدوات تعلم الذكاء الاصطناعي يومياً لتحديد فجوات التعلم الناشئة وتعديل خطط الدروس القادمة وفقاً لذلك
5. استخدام بيانات الأداء لتوجيه لقاءات 1:1 والتدخلات في المجموعات الصغيرة. يجب أن تُرشد بيانات الذكاء الاصطناعي، لا أن تحل محل، الحكم المهني للمعلم بشأن تقدم الطالب.
6. تنبيه قائد رفاه الطالب)أثناء التعلم عن بعد (أو منسق حماية الطفل)أثناء التعلم الحضوري (فوراً إذا أظهر الطالب ضيقاً، أو أفكار إيذاء النفس، أو إفصاحات عن إساءة، أو رسائل غير ملائمة بجدية عبر تفاعلات الذكاء الاصطناعي.
7. مراقبة الإفراط في الاعتماد على الذكاء الاصطناعي)تفريغ العبء المعرفي(، مثل التسليمات الحرفية أو تخطي الاستدلال، ومعالجته من خلال تعزيز توقعات الجهد الحقيقي.

الملحق د .المتطلبات الفنية

حماية البيانات والخصوصية

يجب على المدارس جمع البيانات الشخصية ومعالجتها وتخزينها ومشاركتها والاحتفاظ بها والتخلص منها بصورة قانونية وعادلة وشفافة وآمنة .وبناءً على ذلك، يجب على المدارس تنفيذ ما يأتي:

1. خطة حماية البيانات :توضح فئات البيانات الشخصية المصرح بجمعها ومعالجتها، وإجراءات الحصول على موافقة أولياء الأمور)عند اللزوم(، ومتطلبات تصنيف البيانات وتفويض الوصول، ومتطلبات الاحتفاظ بالبيانات والنسخ الاحتياطي والاسترداد والتخلص منها، والشروط والضمانات المتعلقة بمشاركة البيانات الشخصية مع أطراف ثالثة.
2. عملية الموافقة ومشاركة البيانات :تشمل متطلبات السرية وعدم الإفصاح وحماية البيانات في الاتفاقيات مع الأطراف الثالثة التي تعالج البيانات الشخصية، بما في ذلك الحصول على موافقة كتابية من ولي الأمر)كجزء من اتفاقية ولي الأمر والمدرسة (لجميع الأدوات الرقمية التي قد تستخدمها المدرسة والتي تجمع أو تعالج أو تخزن البيانات الشخصية للطلاب.
3. أدوات الطلاب الرقمية وأدوات الذكاء الاصطناعي :يجب أن تكون هناك موافقة منفصلة وصريحة مطلوبة لأدوات تعلم الذكاء الاصطناعي، مع إبلاغ أولياء الأمور بوضوح بالغرض من استخدام البيانات الشخصية للطلاب وتخزينها ومشاركتها، وبإمكانية الانسحاب)مع ترتيبات تعلم بديلة .(لا يجوز للأدوات استخدام البيانات الشخصية للطلاب لأغراض تجارية، أو للتنميط، أو للمشاركة غير المصرح بها مع أطراف ثالثة، أو لتدريب نماذج الذكاء الاصطناعي، ويجب أن تحذف أو تجعل البيانات الشخصية للطلاب مجهولة الهوية خلال 90 يوماً من مغادرة الطالب للمدرسة، مع تأكيد كتابي من مزود الخدمة عند الطلب.

الأمن السيبراني

،يجب على المدارس تنفيذ وصيانة تدابير الأمن السيبراني التي تحمي الأنظمة الرقمية، وأصول المعلومات، والمستخدمين من الوصول غير المصرح به، وسوء الاستخدام والفقدان، والتعطل، والتهديدات السيبرانية، بما في ذلك:

1. ضوابط الوصول :المصادقة متعددة العوامل عبر الخدمات الحرجة وضوابط الوصول القائمة على الأدوار المحددة/المطبقة لضمان حصول المستخدمين على الأذونات المناسبة.
2. .تشفير البيانات :تشفير البيانات أثناء النقل وعند السكون لحماية المعلومات الحساسة
3. أمن الشبكة :جدران حماية من الجيل التالي وأنظمة كشف/منع التسلل للحماية من الوصول غير المصرح به، مع ضمان إنفاذ سياسات ترشيح الويب، والقدرة على حظر المحتوى غير الملائم وكشف الأجهزة المصابة عبر الشبكة، وجدران حماية قائمة على الهوية لرؤية تفصيلية لنشاط تصفح المستخدمين، وبنية حافة أمنية موحدة لجميع تصفح الإنترنت.
4. حماية نقاط النهاية :برامج مكافحة الفيروسات/البرمجيات الخبيثة المحدثة لجميع الأجهزة التي تديرها المدرسة وتشفير أقراص الأجهزة الصلبة)مع ضمان التصحيح الأمني المنتظم(.
5. النسخ الاحتياطي للبيانات والاسترداد :تنفيذ إجراءات نسخ احتياطي منتظمة وآلية للبيانات الحرجة والبرمجيات وإعدادات التهيئة بما يتماشى مع سياسة سجلات المدارس لدى دائرة التعليم والمعرفة فيما يتعلق بالتكرار والفترة الزمنية المناسبة)مع ضمان حفظ النسخ الاحتياطية في خزائن وتخزينها دون اتصال وبأمان وبشكل منفصل عن شبكة المدرسة(، وخطة قوية للتعافي من الكوارث لتقليل وقت التعطل في حالة وقوع حادث أمني، وبيانات متزامنة مع السحابة للمدارس التي تستخدم أنظمة سحابية خارجية للتخزين.
6. .أمن البيانات :ضوابط تصنيف البيانات عبر بيانات المدرسة والطلاب، مع أدوات منع فقدان البيانات للحماية من تسرب البيانات أو إخراجها غير المصرح به
7. .التدريب على الوعي الأمني :تدريب منتظم للموظفين والطلاب لرفع الوعي بالتهديدات السيبرانية وأفضل الممارسات

8. خطط الاستجابة للحوادث واستمرارية الأعمال :خطط محدثة لمعالجة الخروقات الأمنية بسرعة وفعالية، وتنفيذ محاكاة مكتبية لهجوم سيبراني وتمرين بمشاركة إدارة المدرسة، وتوجيه الموظفين حول عملية الحفاظ على استمرارية الأعمال.
9. الأمن المادي :تأمين الوصول إلى الخوادم المادية، ومعدات الشبكات، والبنية التحتية الحرجة الأخرى.
10. الامتثال التنظيمي :الامتثال للوائح والمعايير المحلية والدولية لحماية البيانات.
11. المراقبة والتسجيل :أنظمة مراقبة شاملة لكشف الحوادث الأمنية والاستجابة لها في الوقت الحقيقي، مع الاحتفاظ بسجلات مفصلة لأغراض التدقيق والتحليل.
12. تطوير البرمجيات الآمن :ممارسات ترميز آمنة عند تطوير أو شراء البرمجيات التعليمية، وتحديث البرمجيات وتصحيحها بانتظام لمعالجة الثغرات.
13. أمن السحابة :في حال استخدام خدمات سحابية، ضمان التزام المزودين المختارين بمعايير أمنية صارمة. تنفيذ التهيئة المناسبة وضوابط الوصول للموارد السحابية، السحابية SaaS مع خدمات هوية المدرسة حيثما أمكن، وإنشاء قدرات إدارة وضعية أمن (SaaS) ودمج الخدمات السحابية - البرمجيات كخدمة.
14. أمن التعاون :منصات اتصال وتعاون آمنة لحماية المعلومات التعليمية الحساسة المشتركة بين الطلاب والموظفين.
15. أمن الأطراف الثالثة :تدقيق ومراقبة موردي الأطراف الثالثة الذين يقدمون حلول التكنولوجيا التعليمية لضمان استيفائهم معايير الأمن.
16. صيانة النظام :صيانة وتحديث البنية التحتية الرقمية وأنظمة التشغيل وأنظمة الأمن والبرمجيات بانتظام، بما في ذلك برامج الحماية من الفيروسات، واختبارها بانتظام لضمان حالة عمل جيدة.
17. الاستخدام الآمن لتطبيقات التعلم الخارجية :وجود آليات صون)مثل أنظمة تسجيل الدخول الموحد (لحماية أمن الطلاب والنظام عند استخدام تطبيقات التعلم الخارجية.

الملحق هـ .عناصر الاستخدام المسؤول والصون

1. التطور المعرفي :يجب على المدارس ضمان أن استخدام الذكاء الاصطناعي والتكنولوجيا القائم في المدرسة يخدم غرضاً تعليمياً واضحاً، وأن تكون هناك استراتيجيات لحماية القدرة المعرفية للطلاب وفاعليتهم واستقلاليتهم وتطويرها، وألا يتيح تفريغ العبء المعرفي الذي يقوض التعلم.
2. النزاهة الأكاديمية :يجب على المدارس التحقق من أن استخدام الذكاء الاصطناعي والتكنولوجيا يدعم النزاهة الأكاديمية ولا يقوض صلاحية التقييمات أو موثوقيتها أو عدالتها، بما يتماشى مع سياسة التقييم والمرسوم بقانون اتحادي رقم 33 لسنة 2023 بشأن مكافحة الغش والإخلال بأنظمة الامتحانات.
3. الرقابة البشرية :يجب على المدارس ضمان وجود رقابة بشرية ذات معنى على أي قرار مدعوم بالذكاء الاصطناعي يؤثر في المسار التعليمي للطالب أو حقوقه أو رفاهه، مع قيام موظف معين بمراجعة القرار النهائي وممارسة الحكم المهني بشأنه والتوقيع عليه.
4. سلامة المحتوى والاعتبار الثقافي :يجب على المدرسة صون الطلاب من خلال التحقق من أن أدوات الذكاء الاصطناعي والتكنولوجيا لا تعرض الطلاب لمحتوى غير مناسب للعمر أو لمحتوى لا يمتثل لسياسة الاعتبار الثقافي.
5. التحيز الخوارزمي والإنصاف :يجب على المدارس تحديد التحيز في أدوات الذكاء الاصطناعي وتقييمه ورصده ومعالجته لضمان مخرجات عادلة وشاملة ومناسبة ثقافياً لجميع الطلاب والموظفين، بما في ذلك تعليم موظفي التدريس والطلاب كيفية التعرف على التحيز.

التعريفات

المصطلح	التعريف
الفاعلية	قدرة الأفراد على اتخاذ قرارات مستنيرة، وممارسة الاستقلالية والسيطرة، والاحتفاظ بمشاركة ذات معنى في الإجراءات والنتائج، بما في ذلك القدرة على فهم استخدام أنظمة الذكاء الاصطناعي وتأثيرها ومساءلتها والتأثير فيهما)اليونسكو، 2023(.
محو الأمية في الذكاء الاصطناعي	المعرفة التقنية، والمهارات المستدامة، والاتجاهات الجاهزة للمستقبل اللازمة للازدهار في عالم يتأثر بالذكاء الاصطناعي. وهو يمكّن المتعلمين من التفاعل مع الذكاء الاصطناعي، والإنشاء به، وإدارته، وتصميمه، مع التقييم النقدي لفوائده ومخاطره وآثاره الأخلاقية)منظمة التعاون الاقتصادي والتنمية، 2025(.
أداة تعلم الذكاء الاصطناعي	نظام تعلم شخصي مدعوم بالذكاء الاصطناعي يكيف المحتوى، ومستوى الصعوبة، و/أو الوتيرة وفقاً لاحتياجات الطلاب)بناءً على أدائهم، ومشاركتهم، و/أو تقدمهم(.
التحيز الخوارزمي	مخرجات منهجية وغير عادلة تنتجها أنظمة الذكاء الاصطناعي نتيجة بيانات متحيزة، أو اختيارات تصميم، أو ممارسات نشر)اليونسكو، 2021(.
الذكاء الاصطناعي (AI)	أنظمة قائمة على الحاسوب مصممة لأداء مهام تتطلب عادةً ذكاءً بشرياً، مثل التعرف إلى الأنماط، واتخاذ القرارات، والتعلم من الخبرة، وتوليد المحتوى (اليونسكو، 2021).
الاستقلالية	قدرة الأفراد على الاحتفاظ بالسيطرة على القرارات والإجراءات، واتخاذ اختيارات مستنيرة، وممارسة الحكم المستقل عند التفاعل مع أنظمة الذكاء الاصطناعي، بما يضمن أن يدعم الذكاء الاصطناعي، لا أن يتجاوز، اتخاذ القرار البشري والمسؤولية والفاعلية، ولا سيما في السياقات التعليمية)اليونسكو، 2021(.
إحضار جهازك الخاص (BYOD)	ممارسة تسمح بموجبها المدارس للموظفين و/أو الطلاب بأداء عملهم على أجهزة رقمية مملوكة لهم شخصياً.
حماية البيانات	عملية صون البيانات من التلف أو الاختراق أو الوصول غير المصرح به أو الفقدان، وتوفير القدرة على استعادة البيانات إلى حالة وظيفية إذا حدث شيء يجعل البيانات غير قابلة للوصول أو غير قابلة للاستخدام (SNIA، دون تاريخ).
حادث رقمي	أي حادث داخلي أو خارجي ينطوي على الاستخدام غير الملائم للتكنولوجيا الرقمية ويؤثر سلباً في أنظمة المدرسة و/أو مجتمعها. ويشمل ذلك خرق سياسات الاستخدام المعقول، أو حادثاً سيبرانياً، أو الوصول إلى محتوى غير ملائم، أو سلوكيات أو اتصالات غير ملائمة، أو تنمراً إلكترونياً، و/أو أي خرق آخر للوائح المدرسة في بيئة رقمية.
الاستخدام المسؤول	الاستخدام الحذر والمدروس والواعي بالمخاطر للأدوات والأنظمة الرقمية من قبل الطلاب والموظفين وقادة المدارس في البيئات التعليمية، بطرق تعظم الفوائد التعليمية مع ضمان السلامة والصون والتقييم المناسب للمخاطر والفوائد قبل الاعتماد)وزارة التعليم في المملكة المتحدة، 2025(.

دائـرة التـعـلـيـم والـمـعـرفـة
DEPARTMENT OF EDUCATION AND KNOWLEDGE

AI & TECHNOLOGY POLICY

UAE School Inspection Framework Alignment

This policy aligns with the UAE School Inspection Standard 4.1 Curriculum Design and Implementation: Elements 4.1.1 Rationale, Balance and Compliance and 4.1.4 Cross-curricular Links and Standard 5.1 Health and Safety, Including Arrangements for Child Protection/Safeguarding: Element 5.1.2 Arrangements to Ensure Health, Safety and Security.

Policy

1. AI and Digital Literacy

1.1 **Curriculum Integration**: Schools shall develop students' AI and digital literacy through their curriculum with increasing technical complexity, in line with Appendix A. AI Literacy Requirements.

1.2 **AI Learning Outcomes Monitoring and Reporting**: Schools shall adopt a Learning Management System (LMS) that integrates AI standards and learning outcomes, ensuring that student AI literacy data is accessible to ADEK for regulatory monitoring.

1.3 **AI Literacy Assessment**: Schools shall ensure that every student graduates with demonstrated AI literacy, assessed through students' application of knowledge and skills in authentic, real-world contexts and adapted for students with additional learning needs, in line with the *Inclusion Policy*.

2. AI Learning Tools

2.1 **AI-Powered Personalized Learning**: Schools shall implement at least one of the AI-powered personalized learning tools ("AI learning tools" including chat or non-chat-based AI tutors) that meet the requirements of Appendix B. AI Learning Tool Criteria and obtain ADEK approval before deploying any tool by completing the "ADEK AI Learning Tool Vetting Form". Schools shall set screen time limitations to maximize learning.

2.2 **Foundational "AI for Teaching" Competency**: Schools shall ensure all relevant teaching and teaching support staff complete foundational training on the use of AI learning tools to identify students' strengths and weaknesses and adapt teaching methods to address learning gaps, in line with Appendix C. Pedagogical Requirements for the Use of AI Learning Tools.

2.3 **AI Learning Tool Training for Students:** Schools shall train all students on the use of their deployed AI learning tools, ensuring students' ability to navigate the tool, use the tool to support their own learning, prompt (if applicable), abide by safety guardrails, and engage in responsible use.

3. Institutional Readiness

3.1 **Digital Strategy**: Develop and implement an annual school-wide digital strategy for the use of AI and technology to improve student achievement, teaching pedagogy, and school operations.

3.2 **Continuous Professional Development (CPD) in AI**: Schools shall ensure staff attendance at all ADEK-mandated training (general and role-specific, when applicable). Staff shall be provided CPD opportunities in human-centered AI use, ethical and responsible AI practices, AI systems and applications, AI-enabled pedagogy, AI for professional growth and improvement, and cybersecurity and digital safety.

3.3 **Digital Infrastructure and Systems:** Schools shall maintain reliable digital infrastructure and systems (e.g., networks, applications, devices, and services), in line with Appendix D. Technical Requirements, including but not limited to secure school-issued devices and safety measures for Bring Your Own Device (BYOD) arrangements, staff access to digital systems and platforms provided by ADEK, readiness for ADEK-approved distance learning, and any assistive technologies, in line with the *Inclusion Policy*.

4. Responsible Use

4.1 **Responsible Use Policies**: Schools shall regulate the responsible use of AI and technology to protect and maximize learning, ensure ethical academic behavior and oversight, and safeguard user wellbeing, including the requirements in Appendix E. Responsible Use and Safeguarding Elements through age- and culturally-appropriate policies for students, staff, parents, and other users.

4.2 **Student Phone Usage**: Students shall not be authorized to use personal mobile phones on school premises during the school day (unless explicitly and exceptionally authorized by a teacher for learning purposes). Schools shall ensure other SIM-enabled devices (e.g., smart watches) are communication-disabled and that devices necessary for learning (e.g., tablets, laptops) are only used for learning purposes and actively monitored to prevent distraction.

4.3 **Student Social Media Usage**: Schools shall not authorize students to use social media, in line with Cabinet Resolution No. (106) of 2026 Regarding the Regulation of Children's Access to Social Media and its amendments.

4.4 **Virtual Private Networks (VPNs) Usage**: Schools shall not authorize the use of VPNs on any device on school premises and networks.

4.5 **Parent Partnership**: Schools shall regularly inform parents of their obligation to monitor their child's digital behavior outside school and limit social media use for children aged 15 and under, in line with Federal Decree Law No. 26 of 2025 on Child Digital Safety and Cabinet Resolution No. (106) of 2026 Regarding the Regulation of Children's Access to Social Media and their amendments.

5. Security

5.1 **Vendor Selection**: Schools shall establish procedures for selecting and managing external technology vendors, products, and services that meet ADEK requirements and UAE laws.

5.2 **Digital Incidents**: Schools shall identify, manage, document, respond to, and report digital incidents, supporting affected students and informing parents as applicable, in line with *Student Protection Policy*, *Student Behavior Policy*, *Records Policy*, and applicable UAE laws.

5.3 **Data Protection and Cybersecurity**: Schools shall implement and maintain data protection and cybersecurity measures, in line with Appendix D. Technical Requirements, Federal Decree Law No. 45 of 2021 on the Protection of Personal Data, Federal Decree Law No. 34 of 2021 on Combatting Rumors and Cybercrimes, and Federal Decree Law No. 26 of 2025 on Child Digital Safety, and their amendments, and any other laws and requirements issued by relevant government authorities.

5.4 **Digital Communication and Social Media**: Schools shall implement the secure storage and appropriate use of digital media, establish controls for official school social media accounts, monitor official and unofficial school-related communication channels, and obtain parental consent before recording or publishing identifiable student digital media.

5.5 **Staff Personal Communication Practices**: Schools shall inform staff of unauthorized practices, including the use of personal email or social media accounts to communicate with current students, former students aged below 18, or parents, or the use of personal social media accounts to disseminate confidential school information or content that may be inappropriate, discriminatory, harmful, or perceived as endorsed by the school.

6. Communications

6.1 **School Website**: Schools shall maintain an updated school website containing all ADEK-mandated information.

Compliance

Schools are expected to be fully compliant with this policy by AY 2027/28 (Fall term).

Failure to comply with this policy shall be subject to legal accountability and the penalties stipulated in accordance with the ADEK's regulations, policies, and requirements, notwithstanding any other penalties imposed by Federal Decree Law No. (31) of 2021 Promulgating the Crimes and Penalties and its amendments or any other relevant law. ADEK reserves the right to intervene if the school is found to be in violation of its obligations.

Expected Outcomes

ADEK will assess the impact of this policy through the following expected outcomes:

1. Improved AI and digital literacy among students
2. Strengthened AI-enabled pedagogy among teachers
3. Improved student learning outcomes (attainment and progress) using AI learning tools
4. Enhanced responsible use of AI and technology in schools

Appendix A. AI Literacy Requirements

Schools shall implement the *ADEK K-12 AI Literacy Framework* as follows:

1. **Integrating AI Literacy into the Curriculum**: Schools shall ensure students develop the four interconnected AI literacy strands through their curriculum: AI Conceptual Understanding; Critical Evaluation and Informed Interaction; AI Creation, Engineering, and System Design; and Responsible Governance, Data Privacy, and Societal Impact.

2. **AI Learner Profiles and Phasing**: Schools shall introduce the four AI literacy strands across four developmental phases and learner profiles, progressing with increasing technical complexity. The core competencies that students should aim to meet for each of the four AI learner profiles are defined in Table 1. AI Learner Profiles and Phases:

Table 1. AI Learner Profiles and Phases

Phase/Cycle	AI Learner Profile	Core Competency Milestone
Phase 1/KG: KG1–KG2/FS2-Year 1	**AI Aware Explorer**	**Explores inputs and responses through play** Students distinguish between human senses and basic machine inputs and understand cause-and-effect relationships. Learning is unplugged with no direct AI tool use.
Phase 2/Cycle 1: Grades 1–5/Year 2-6	**AI Literate Thinker**	**Applies rules, logic, and data to generate and evaluate outputs.** Students progress from rule-based thinking to multi-step logic, develop understanding of how data influences outcomes, and begin interacting with AI tools to refine outputs.
Phase 3/Cycle 2: Grades 6–8/Year 7-9	**AI Solution Builder**	**Designs and improves AI-powered solutions using data, models, and workflows.** Students build, evaluate, and refine solutions using structured processes and foundational ML concepts.
Phase 4/Cycle 3: Grades 9–12/ Year 10-13	**AI Systems & Solutions Designer**	**Designs and governs integrated AI systems.** Students develop real-world solutions using systems thinking and ensure effectiveness, responsibility, and alignment with societal and governance expectations.

3. **Learning Objectives and Competencies**: Schools shall adopt a spiral learning design for their AI curriculum, revisiting foundational concepts with increasing complexity across grades.

4. **Mode of Integration**: Schools shall integrate AI literacy into their curriculum using one of the following modes:

    a. Stand-alone: AI is taught as a single, stand-alone unit or module as part of a dedicated ICT subject (e.g., Computer Science, Technology, ICT, etc.) with a specified minimum number of credit hours each year for each phase.

    b. Embedded: AI is embedded in multiple subjects and topics, rather than limited to stand-alone subjects (e.g., AI in Math, Science, etc.), to support authentic learning experiences and the application of AI understanding in real-world and interdisciplinary contexts.

c. Hybrid: AI is taught both through the school's dedicated ICT subject and also embedded across multiple subjects and topics.

Appendix B. AI Learning Tool Criteria

Schools shall apply Table 1. Mandatory AI Learning Tool Criteria when evaluating AI learning tools. Schools seeking ADEK approval for a tool shall submit evidence against each criterion through the "ADEK AI Learning Tool Request Form." Approval will only be granted to tools that meet all mandatory criteria.

Table 1. Mandatory AI Learning Tool Criteria

Criterion	Evaluation Questions and Requirements
Safety and Self-Harm Detection	1. Does the tool detect expressions of self-harm, suicidal ideation, abuse, or severe distress (if applicable)? 2. Upon detection, does it immediately alert the teacher and/or the school administrator (if applicable)? 3. Does the tool allow teachers to customize safety/self-harm guardrails through prompting and/or configuration features?
Cultural Content Filtering	1. Does the tool detect and filter out culturally inappropriate content through chat-based customization or configuration set-up? Culturally inappropriate content includes: • human reproduction and evolution dogma • alternative gender identity and sexual orientation • alcohol and drugs • religious/political indoctrination 2. Does the tool alert the teacher and/or the administrator?
Academic Integrity	1. Does the tool detect and block plagiarism attempts?
Teaching Pedagogy	2. Does the tool employ evidence-based pedagogical approaches, including one or more of: • Socratic questioning (guiding students to answers through probing) • mastery learning (requiring proficiency before advancing) • spaced repetition (scheduling review at intervals for long-term retention) • retrieval practice (testing recall rather than re-reading) 3. Does it guide students to think and reason rather than simply providing answers?
Curriculum and Content Integration	1. Does the tool integrate your school's curriculum standards (e.g., UAE Ministry of Education (MoE), UK National, US Common Core, International Baccalaureate (IB), and CBSE)? OR Can the school or teacher upload customized standards/learning outcomes? 2. Does the tool link/tag and report on the mastery of curriculum standards/learning outcomes
Assessment and Learning Resources	1. Does the tool provide pre- and post- assessments capturing students' learning outcomes at the start and end of each unit? 2. Can the teacher use the tool to generate customized lesson plans, presentations, practice sets, quizzes, differentiated tasks,

	and formative assessment items aligned to their curriculum standards and class needs (if applicable)? 3. Can the teacher edit, adapt, or reject AI-generated content before publishing to students (if applicable)?
Teacher Interface: Student-Level Activity	1. Can the teacher view all of the below for each individual student: • learning gaps • student engagement • time spent on tool • completion progress for assigned tasks • completion rates for assigned tasks • student attainment by learning outcome • student progress by learning outcome • full conversation log/chat history (if applicable) • performance trends over time 2. Are learning concerns identified to the teacher? 3. Does the tool generate detailed progress reports showing mastery trends over time?
Teacher Interface: Class-Level Activity	• Can the teacher view class-level analytics including all of the below: • learning gaps • student engagement • time spent on tool • completion progress for assigned tasks • completion rates for assigned tasks • performance trends over time • comparison of individual student performance against the class baseline
Administrator Access	1. Can the school administrator view: • teacher usage and interactions with the tool • student engagement • student completion of assigned tasks • full conversation log (chat history) for students flagged on safety, self-harm, and cultural inappropriateness (if applicable) 2. Can the administrator manage user accounts, permissions, and tool configurations at school level? 3. Can ADEK be granted system-level administrative access to conduct quality assurance reviews?

Guardrail Prompt for AI Learning Tools

Teachers shall copy/paste or embed this prompt within the AI learning tool interface, including in chat instructions for class and space creation, lesson and assignment generation, and/or system prompt settings to guide and constrain the AI's responses before student interaction.

> *Prompt:*
> *You are an AI tutor configured for use in UAE schools. You must comply with UAE cultural and legal norms at all times.*
>
> *Core rules:*

1. *Restrict all responses to the assigned lesson topic only.*
2. *Decline any questions about human reproduction and evolution dogma, alternative gender identity and sexual orientation, alcohol and drugs, religious/political indoctrination.*
3. *Do not provide any contact numbers for support to students in any case.*
4. *For any child protection or safeguarding concerns detected, encourage students to reach out to a teacher, principal, school counselor, or other responsible adult.*
5. *Never engage with anything that could harm a student. Always direct concerns to a trusted adult or school counselor.*
6. *Encourage respectful, positive communication. Calmly redirect rude or off-topic messages back to the lesson.*
7. *Reflect UAE values in every response. Avoid anything that conflicts with Islamic values or UAE norms. Never criticize any religion, culture, or nationality.*
8. *When food comes up, promote healthy, balanced eating. Never reference foods prohibited under Islamic dietary guidelines. Support positive body image.*

Appendix C. Pedagogical Requirements for the Use of AI Learning Tools

Teachers and teaching assistants using AI learning tools shall meet the following requirements:

Curriculum Alignment:

1. Ensure guardrails for safety and cultural appropriateness are in place for safety, self-harm, and cultural appropriateness using the prompt outlined in Guardrail Prompt for AI Learning Tools (Appendix B).
2. Assign age-appropriate learning tasks that are directly aligned to the curriculum standards/learning outcomes.
3. Adapt tasks by ability level to ensure all students, including those with additional learning needs, receive tasks appropriate to their skill level.

Content and Lesson Generation:

1. Generate lesson plans, presentations, practice sets, and differentiated learning materials using AI learning tools.
2. Verify factual accuracy and ensure curriculum alignment of AI-generated lesson plans and resources.

Monitoring Student Learning:

1. Screen and monitor student- and class-level performance utilizing the AI learning tool to identify learning gaps and introduce interventions, as needed:
   a. If a majority of students are showing learning gaps on a specific concept (e.g., calculating areas under curves, understanding how enzymes work, writing using active voice), cover these concepts in more details during the subsequent synchronous lessons to close the gap at the class-level (Tier 1).
   b. If only one or a few students are having difficulties, teachers shall provide more targeted 1:1 or small-group interventions (Tier 2 or 3) as required (e.g., brief 5-minute sessions through individual office hours, a synchronous 5-10 minute sub-session for the target group or individual while the rest of the class is working on asynchronous work).
2. Reconfigure the AI learning tool to test whether students have understood the concepts and to validate if the intervention was effective in closing the learning gaps.
3. Review student-level data on AI learning tools weekly to ensure student engagement and completion of assignments, while monitoring off-topic inappropriate content on the AI learning tool.

4. Review overall class-level student data on AI learning tools daily to identify emerging learning gaps and adjust upcoming lesson plans accordingly.
5. Use performance data to guide 1:1 check-ins and small-group interventions. AI data should inform, not replace, teacher professional judgement about a student's progress.
6. Alert the Student Welfare Lead (during distance learning) or Child Protection Coordinator (during on-site learning) immediately if a student shows distress, self-harm ideation, abuse disclosures, or seriously inappropriate messaging via AI interactions.
7. Monitor for over-reliance on AI (cognitive offloading), such as verbatim submissions or skipped reasoning, and address it by reinforcing expectations for genuine effort.

Appendix D. Technical Requirements

Data Protection and Privacy

Schools shall collect, process, store, share, retain, and dispose of personal data lawfully, fairly, transparently, and securely. Accordingly, schools shall implement the following:

1. **Data Protection Plan**: Outlining the categories of personal data authorized for collection and processing, procedures for obtaining parental consent (where required), data classification and access authorization requirements, data retention, backup, recovery, and disposal requirements, and conditions and safeguards for sharing personal data with third parties.
2. **Consent and Data Sharing Process**: Including confidentiality, non-disclosure, and data protection requirements in agreements with third parties that process personal data, including obtaining written parental consent (as part of the Parent School Agreement) for all digital tools that the school may use that collects, processes, or stores student personal data.
3. **Student Digital and AI Tools**: Separate, explicit consent shall be required for AI learning tools, clearly informing parents regarding the purpose, use, storage, and sharing of student personal data, and the ability to opt out (with alternative learning arrangements). Tools shall not use student personal data for commercial purposes, profiling, unauthorized third-party sharing, or AI model training, and shall delete or anonymize student personal data within 90 days of a student leaving the school, with written confirmation from the service provider upon request.

Cybersecurity

Schools shall implement and maintain cybersecurity measures that protect digital systems, information assets, and users from unauthorized access, misuse, loss, disruption, and cyber threats, including:

1. **Access Controls**: Multi-factor authentication across critical services and defined/enforced role-based access controls to ensure users have appropriate permissions.
2. **Data Encryption**: Encryption for data in transit and at rest to safeguard sensitive information.
3. **Network Security**: Next-generation firewalls and intrusion detection/prevention to protect against unauthorized access, ensuring enforcement of web filtering policies, ability to block inappropriate content and detect infected machines across the network, identity-based firewalls for granular visibility on user browsing activity, unified security edge architecture for all internet browsing.
4. **Endpoint Protection**: Updated anti-virus/malware software of all school-managed devices and hard disk device encryption (ensuring regular security patching).
5. **Data Backup and Recovery**: Automated regular backup procedures for critical data, software, and configuration settings are performed in line with the ADEK School Records Policy with regard to frequency and appropriate period of time (ensuring backups are vaulted and stored offline, securely and separately from the school network), a robust disaster recovery plan to minimize downtime in case of a security incident, and cloud-synced data for schools that use external cloud systems for storage.
6. **Data Security**: Data classification controls across school and student data, with Data Loss Prevention Tools to protect against data leaks or exfiltration.
7. **Security Awareness Training**: Regular training for staff and students to raise awareness about cybersecurity threats and best practices.
8. **Incident Response and Business Continuity Plans**: Updated plans to address security breaches promptly and effectively, performing a tabletop cyber-attack simulation and

exercise with school management involvement, and guiding staff on process for maintaining business continuity.
9. **Physical Security**: Secure access to physical servers, networking equipment, and other critical infrastructure.
10. **Regulatory Compliance**: Compliance with local and international data protection regulations and standards.
11. **Monitoring and Logging**: Comprehensive monitoring systems to detect and respond to security incidents in real time, maintaining detailed logs for auditing and analysis purposes.
12. **Secure Software Development**: Secure coding practices when developing or procuring educational software, regularly update and patch software to address vulnerabilities.
13. **Cloud Security**: If using cloud services, ensure the selected providers adhere to stringent security standards. Implement proper configuration and access controls for cloud resources, integrating Cloud Services – Software as a Service (SaaS) with school identity services where possible, and establish Cloud SaaS Security Posture Management capabilities.
14. **Collaboration Security**: Secure communication and collaboration platforms to protect sensitive educational information shared among students and staff.
15. **Third-Party Security**: Vet and monitor third-party vendors providing educational technology solutions to ensure they meet security standards.
16. **System Maintenance**: Regularly maintained and updated digital infrastructure, operating systems, security systems, and software, including antivirus protection software, tested regularly to ensure good working condition.
17. **Safe Use of External Learning Applications**: Safeguarding mechanisms in place (e.g., single sign-on systems) to protect student and system security in the use of external learning applications.

Appendix E. Responsible Use and Safeguarding Elements

1. **Cognitive Development**: Schools shall ensure school-based AI and technology use serves a clear educational purpose and that strategies are in place to protect and develop students' cognitive ability, agency, and autonomy, and does not enable cognitive offloading that undermines learning.
2. **Academic Integrity**: Schools shall verify that the use of AI and technology supports academic integrity and does not undermine the validity, reliability, or fairness of assessments, in line with the *Assessment Policy* and the Federal Decree Law No. 33 of 2023 Concerning Combating Cheating and Violation of Examination Systems.
3. **Human Oversight**: Schools shall guarantee meaningful human oversight of any AI-supported decision affecting a student's educational path, rights, or wellbeing, with a designated staff member reviewing, exercising professional judgement on, and signing off on the final decision.
4. **Content Safety and Cultural Consideration**: School shall safeguard students by verifying that AI and technology tools do not expose students to age-inappropriate content or to content that does not comply with the *Cultural Consideration Policy*.
5. **Algorithmic Bias and Fairness**: Schools shall identify, evaluate, monitor, and address bias in AI tools to ensure fair, inclusive, and culturally appropriate outcomes for all students and staff, including teaching staff and students how to recognize bias.

Definitions

Agency	The capacity of individuals to make informed decisions, exercise autonomy and control, and retain meaningful involvement in actions and outcomes, including the ability to understand, question, and influence the use and impact of AI systems (UNESCO, 2023).
AI Literacy	The technical knowledge, durable skills, and future ready attitudes required to thrive in a world influenced by AI. It enables learners to engage, create with, manage, and design AI, while critically evaluating its benefits, risks, and ethical implications (OECD, 2025).
AI Learning Tool	An AI-powered personalized learning system that adapts content, difficulty level, and/or pacing according to students' needs (based on their performance, engagement, and/or progress).
Algorithmic Bias	Systematic and unfair outcomes produced by AI systems as a result of biased data, design choices, or deployment practices (UNESCO, 2021).
Artificial Intelligence (AI)	Computer-based systems designed to perform tasks that normally require human intelligence, such as recognising patterns, making decisions, learning from experience, and generating content (UNESCO, 2021).
Autonomy	The ability of individuals to retain control over decisions and actions, make informed choices, and exercise independent judgement when interacting with AI systems, ensuring that AI supports, rather than overrides, human decision-making, responsibility, and agency, particularly in educational contexts (UNESCO, 2021).
Bring Your Own Device (BYOD)	Practice wherein schools allow staff and/or students to do their work on personally owned digital devices.
Data Protection	The process of safeguarding data from corruption, compromise, unauthorized access, or loss and providing the capability to restore the data to a functional state should something happen to render the data inaccessible or unusable (SNIA, n.d.).
Digital Incident	Any internal or external incident involving the inappropriate use of digital technology that negatively impacts the school's systems and/or community. This includes a breach of the reasonable usage policies, a cybersecurity incident, the accessing of inappropriate content, inappropriate behaviors or communications, cyberbullying, and/or any other breach of school regulations in a digital setting.
Responsible Use	The careful, considered, and risk-aware use of digital tools and systems by students, staff, and school leaders in educational settings, in ways that maximize educational benefits while ensuring safety, safeguarding, and appropriate evaluation of risks and benefits before adoption (UK Department for Education, 2025).