

مقرر ICDL الأمن السيبراني للمربين والمعلمين

إصدار المنهاج ١,٠

الغرض

يهدف هذا المستند إلى تقديم التفاصيل حول منهج ICDL الأمن السيبراني للمربين والمعلمين. يصف المنهج، من خال مخرجات التعليم، المعرفة والمهارات التي يجب أن يمتلكها المرشح للحصول على شهادة ICDL الأمن السيبراني للمربين والمعلمين. كذلك يقوم المنهج بتقديم

حقوق النشر مؤسسة ICDL © 2019

جميع الحقوق محفوظة. لا يجوز إعادة نشر أي جزء من هذا المستند بأي شكل كان، إلا بالحصول على موافقة من مؤسسة ICDL . يجب توجيه الاستفسارات حول الحصول على الموافقة لإعادة نشر المواد إلى مؤسسة ICDL .

إخلاء المسؤولية

بالرغم من أخذ كل عناية من قبل مؤسسة ICDL في إعداد هذا المنشور، لا يتم إعطاء أي ضمان من مؤسسة ICDL ، بصفتها الناشر، حول اكتمال المعلومات الواردة فيه، ولن تتحمل مؤسسة ICDL أية مسؤولية عن أية أخطاء، سهو، عدم دقة، خسارة أو ضرر من أي نوع تنشأ بموجب هذه المعلومات أو أية تعليمات واردة في هذا المنشور. يجوز إجراء تغييرات من قبل مؤسسة ICDL حسب تقديرها الخاص وفي أي وقت ودون إشعار مسبق.

الأمن السيبراني للمربين والمعلمين في التعليم المدرسي (K-12) من رياض الأطفال حتى المرحلة الثانوية

تم تطوير هذا المقرر لإعطاء نظرة شاملة على الأمن الرقمي في المجال التعليمي. تتمثل المحصلة النهائية من هذه الشهادة في التأكد من أن المعلمين وأعضاء هيئة التدريس لديهم فهم قوي للمخاطر التي تحيط بالطلاب الذين يستخدمون الإنترنت، وكيف ينبغي عليهم تحديد ومواجهة هذه المخاطر.

أهداف المقرر

عند إتمام هذا المقرر سيتمكن المرشحون الناجحون من:

- 1- التعرف على المخاطر الأمنية المحتملة وأوجه القصور عند الطلاب المشاركين في مختلف الأنشطة على الإنترنت.
- 2- تطوير وتحديث وعي وفهم المعلمين فيما يتعلق بحماية الطلاب لمساعدتهم في الحفاظ على سلامة الطلاب على الإنترنت.
- 3- فهم كيفية إنشاء خطط فعالة للمساعدة في حماية الطلاب على الإنترنت، بما في ذلك دعم اهتمامات أولياء الأمور.
- 4- استخدام الأدوات والتقنيات المختلفة لتأمين وحماية الطلاب من خلال خبراتهم على الإنترنت.
- 5- معرفة الطرق العملية للحفاظ على سلامة الطلاب على الإنترنت، مثل محركات البحث الآمنة للأطفال، وإعدادات الخصوصية، وبرامج الرقابة الأبوية.
- 6- تطوير الوعي بالمخاطر على الإنترنت، مثل التنمر الإلكتروني، والرسائل غير الملائمة، والتحرش الجنسي، ومواقع الإنترنت ذات المحتوى غير الملائم، والتطرف الإلكتروني، والمشاركة (النشر) على الإنترنت والاستخدام غير الملائم لمواقع التواصل الاجتماعي.
- 7 - التعرف على كيفية مساعدة الطلاب على إدارة الأمن والسلامة على الإنترنت، بما في ذلك التحدث مع الطلاب حول المحتوى والأنشطة الموجودة على الإنترنت.
- 8- فهم التشريعات ذات الصلة والتوجيهات الأخلاقية لحماية الطلاب.
- 9- التعرف على الأنواع المختلفة لمخاطر الإنترنت وعلامات التنمر الإلكتروني، لتوعية الطلاب برد الفعل المناسب عند التعرض لمثل هذه المخاطر.
- 10- فهم سياسات وإجراءات الأمن الرقمي للحفاظ على سلامة الطلاب.
- 11- تتبع التغييرات في سلوك الأطفال على الإنترنت، وتحديثها بالمستجدات والمخاطر الجديدة.
- 12- فهم مجموعة من تدابير السلامة، مثل الوعي والاستراتيجيات والقواعد التي تنظم الاتصال بالإنترنت وطريقة استخدامه. أيضاً بناء المرونة الرقمية للأطفال من خلال السلامة والخصوصية.
- 13- فهم كيفية استخدام سياسات الأمان والموارد المتاحة.
- 14- فهم وتطبيق أساسيات ومبادئ التفكير الأخلاقي على المشاكل المتعلقة بأجهزة الكمبيوتر والتقنيات الرقمية.
- 15- تحديد المشاكل القانونية والتوعية بعواقب خرق الطلاب لقوانين الإنترنت.

يستند هذا المقرر على الخبرات والتجارب الدولية للأمن الرقمي للمعلمين، وخصوصاً مراحل التعليم المدرسي (K-12) من رياض الأطفال حتى المرحلة الثانوية من العديد من الدول الرائدة في مجال التعليم، وتشمل التالي:

- 1- The UK Council for Child Internet Safety (UKCCIS)- Government of UK
- 2- UK Safer Internet Centre
- 3- Research Paper: children's use of the internet – London School of Economics and Political Science (LES)
- 4- Organization Stop it Now- UK and Ireland
- 5- Australian Parenting Website
- 6- Office of the E-safety Commissioner- Government of Australia
- 7- Federal Trade Commission – Protecting American's Consumer – US
- 8- The Privacy Technical Assistance Centre - U.S. Department of Education
- 9- COSN Leading Education Innovation- Norway and Finland Built Innovative, Trusted Educational Environments.
- 10- The K12- Cybersecurity Resource Centre-Department of Education – Ohio - US
- 11- Canada's Centre for Digital and Media Literacy
- 12- National Crime Agency – Child Line – UK
- 13- US News Education
- 14- The Security Awareness Company (SAC) –US
- 15- Office of Education Technology (OET)
- 16- Security Best Practices Guideline for Districts- Kentucky Department of Education
- 17- City University of New York (CUNY) CUNY Academic Works- US
- 18- United Nations Educational, Scientific and Cultural Organization
- 19- Operationally Critical Threat, Asset, and Vulnerability Evaluation is a service mark of Carnegie Mellon University
- 20- Council of the Great City School – Baltimore City Public School – USA
- 21- National Cybersecurity Centre- Government of UK

الموضوع	المهارة	رقم المرجع	نقاط الموضوع
1 استخدام الإنترنت والشبكات الاجتماعية في المدارس	1.1 استخدام الإنترنت	1.1.1	التعرف على فوائد استخدام الإنترنت لدعم وتعزيز عملية التدريس والتعلم.
		1.1.2	إدراك الحاجة إلى توعية الطلاب بالمخاطر التي يمكن التعرض لها عند استخدام الإنترنت، مثل عرض محتوى أو رسائل غير لائقة.
		1.2.1	تحديد الفوائد التعليمية المكتسبة من استخدام التكنولوجيا الرقمية ووسائل التواصل الاجتماعي عند استخدامها بشكل صحيح من قبل المعلمين والطلاب.
	1.2 استخدام وسائل التواصل الاجتماعي	1.2.2	تحديد فوائد استخدام منصات التواصل الاجتماعي لدعم الطلاب في تحميل ومشاركة المحتوى المميز في الصف .
2 مخاطر استخدام الإنترنت	2.1 المخاطر التي تلحق بالطلاب على الإنترنت	1.2.3	إدراك أن وسائل التواصل الاجتماعي يمكنها إشراك الطلاب في المجتمعات الافتراضية الإلكترونية وفقاً للاهتمامات المشتركة.
		1.2.4	تحديد الخطوط العريضة لاستخدام منصات التواصل الاجتماعي المعروفة، مثل Facebook و Instagram و Twitter و Snapchat وغيره.
		2.1.1	إدراك أن تزايد أعداد الطلاب الذين يستخدمون الأجهزة المحمولة للاتصال بالإنترنت يمكن أن ينطوي على فوائد ومخاطر.
		2.1.2	تحديد أنواع المحتوى الموجود على الإنترنت الذي يمكن أن يسبب ازعاجاً للطلاب.
		2.2.1	التعرف على أنواع المخاطر المختلفة التي قد يواجهها الطلاب عند استخدام الإنترنت، وتشمل مخاطر المحتوى ومخاطر الاتصال ومخاطر السلوك.
	2.2 مخاطر أمن الإنترنت بالنسبة للطلاب	2.2.2	الانتباه إلى مخاطر المحتوى التي قد يتعرض لها الطلاب عن غير قصد، وتشمل المواقع الإلكترونية غير اللائقة.
		2.2.3	الانتباه إلى خطر الاستمالة الإلكترونية.
		2.2.4	فهم مخاطر السلوك التي تشمل التنمر الإلكتروني وإرسال الرسائل غير اللائقة.
		2.2.5	تحديد أنواع مخاطر الإنترنت التي قد يواجهها الطلاب، وإدراك أن المخاطر تختلف وفقاً لكيفية تفاعل الطلاب مع البيئة الرقمية.
		3.1.1	التعرف على مواقع التواصل الاجتماعي المعروفة التي قد تشكل خطراً، مثل التعرض للتنمر الإلكتروني وتهديدات الهندسة الاجتماعية.
3 الشبكات الاجتماعية	3.1 مخاطر وسائل التواصل الاجتماعي	3.1.2	فهم مصطلح "البصمة الرقمية"
		3.2.1	فهم أن التواصل مع الطلاب يوفر فرصة لحمايتهم وضماناً لسلامتهم على الإنترنت.
	3.2 نظرة على مخاطر وسائل التواصل الاجتماعي	3.2.2	فهم أن منصات التواصل الاجتماعي تضع قيوداً عمرية على الاستخدام.
		3.2.3	فهم أن حجب أو حظر منصات التواصل الاجتماعي الأساسية ليس حلاً مناسباً حتى للطلاب أصحاب الفئة العمرية الصغيرة.
		3.3.1	فهم أن كتابة دليل استرشادي عن السلوك الذي يجب اتباعه على وسائل التواصل الاجتماعي يمكن أن يساعد الطلاب على استخدام وسائل التواصل الاجتماعي بشكل مسؤول ولائق وآمن.
	3.3 وسائل التواصل الاجتماعي: السلامة الإلكترونية	3.3.2	فهم أن التوجيه السليم يشجع على السلوك الأخلاقي والمواقف والمعتقدات الجيدة، بما في ذلك استخدام الطلاب للتكنولوجيا.
		3.3.3	معرفة كيف تكون مواطناً رقمياً مسؤولاً ومشاركاً في العالم الافتراضي بطريقة أخلاقية ولائقة.

الموضوع	المهارة	رقم المرجع	نقاط الموضوع
		3.3.4	تحديد أفضل الممارسات للشباب عند نشر المحتوى وكتابة التعليقات على الإنترنت.
		3.3.5	التعرف على كيفية إنشاء دليل إرشادي للخصوصية والإعدادات الخاصة بالطلاب واتخاذ القرارات المشتركة حول الأنظمة الأساسية لحماية خصوصيتهم على الإنترنت.
		3.3.6	الانتباه إلى أساسيات الأمان الخاصة بالطلاب عند استخدامهم لمنصات التواصل الاجتماعي.
		3.3.7	فهم كيفية وضع القواعد والإرشادات، دون منع الطلاب من النشر على مواقع التواصل الاجتماعي، مثل مراقبة النطاق العمري.
	3.4 فهم كيف يمكن أن تشكل الأنواع المختلفة من تطبيقات التواصل الاجتماعي خطراً	3.4.1	فهم المخاطر التي يتعرض لها الطلاب من استخدام أنواع معينة من تطبيقات التواصل الاجتماعي، مثل Calculator و live.ME و yubo و blendr.
4 مخاطر وأضرار الإنترنت	4.1 التنمر الإلكتروني	4.1.1	توضيح معنى التنمر الإلكتروني.
		4.1.2	تحديد المشكلات البارزة المرتبطة بنمو مواقع الشبكات الاجتماعية وزيادة مستوى الوعي التكنولوجي بين الطلاب: التنمر الإلكتروني.
		4.1.3	فهم سبب حدوث التنمر الإلكتروني
		4.1.4	التعرف على تأثيرات ومخاطر التنمر الإلكتروني.
		4.1.5	فهم الأشكال المختلفة للتنمر الإلكتروني، وسبب ومكان حدوثها.
		4.1.6	فهم كيفية اكتشاف علامات التنمر الإلكتروني، مثل الأداء الأكاديمي المنخفض، والانسحاب، والسلوك العاطفي والهدام.
		4.1.7	التعرف على طرق لمساعدة الطلاب على تجنب أو تقليل خطر التنمر الإلكتروني.
		4.1.8	فهم كيفية دعم ضحايا التنمر الإلكتروني عن طريق الخطوات: اذهب، تأكد، أخبر، أبلغ، أبدأ واحذف.
		4.1.9	التعرف على دور الوالدين في دعم الطلاب في المنزل.
		4.1.10	فهم كيفية العمل مع مدرسة الطالب في ما يتعلق بالتنمر.
		4.1.11	فهم ما الذي يمكن القيام به إذا طلب الطالب عدم تدخل المدرسة.
		4.1.12	فهم كيفية الترويج لبيئة مدرسية آمنة في حال استمرار وجود التنمر الإلكتروني.
		4.1.13	فهم ما يجب أن يعرفه الطالب فيما يتعلق بالصدقات العدوانية والسامة.
	4.2 الإعلانات على الإنترنت والطلاب	4.2.1	فهم أين تظهر إعلانات الإنترنت للطلاب
		4.2.2	فهم مدى تأثير عمر الطالب على كيفية إدراك إعلانات الإنترنت.
		4.2.3	فهم كيف يمكن للطلاب التعرف على الإعلانات الزائفة والمضللة
	4.3 المواقع الإلكترونية ومقاطع الفيديو غير اللائقة	4.3.1	فهم المقصود بالمواقع الإلكترونية ومقاطع الفيديو غير اللائقة
		4.3.2	التعرف على السلوكيات المختلفة التي قد يقوم بها الطلاب فيما يتعلق بالمواقع الإلكترونية والمحتوى غير اللائق.
		4.3.3	تحديد الأماكن التي قد يواجه فيها الطالب المحتوى غير اللائق.

الموضوع	المهارة	رقم المرجع	نقاط الموضوع
		4.3.4	فهم كيفية التحدث بشكل مناسب مع الطلاب حول المحتوى غير اللائق وكيفية حمايته من هذا على الإنترنت.
		4.3.5	فهم الإرشادات التي يجب اتباعها في حالة تعرض الطالب لمحتوى غير لائق على الإنترنت
		4.3.6	فهم ما يمكن أن يقوم به المعلمين عند اكتشاف أن الطلاب يقومون بتصفح محتوى غير لائق على الإنترنت
	4.4 الرسائل غير اللائقة والتحرش الجنسي	4.4.1	فهم المقصود بإرسال رسائل ومحتوى غير لائق يتضمن مواد إباحية.
		4.4.2	تعريف مصطلح التحرش الجنسي على الإنترنت.
		4.4.3	تعريف مصطلح الاستمالة الإلكترونية (grooming)
		4.4.4	فهم كيفية تمييز الاستغلال الجنسي للأطفال.
		4.4.5	الانتباه إلى سلوكيات الإنترنت التي تنطوي على مخاطر، مثل الصور التي تتم مشاركتها بدون موافقة.
		4.4.6	التعرف على الأسباب التي تجعل من إرسال الرسائل غير اللائقة مشكلة خطيرة للطلاب، وكيف يمكن أن يؤدي ذلك إلى ترك بصمة رقمية والتعرض للتنمر الإلكتروني.
		4.4.7	فهم أهمية التحدث إلى الطلاب حول الرسائل غير اللائقة
		4.4.8	فهم كيفية بدء حوار مع الطلاب حول الرسائل غير اللائقة
		4.4.9	فهم كيف يرد الطالب في حال تلقيه رسالة غير مرغوب فيها أو تتضمن
		4.4.10	التعرف على كيفية تقديم المساعدة للطالب الذي أرسل رسالة غير مرغوب فيها أو تتضمن محتوى إباحي.
		4.4.11	التعرف على الخطوات التي يجب اتخاذها لمساعدة الطالب الذي قام بنشر رسالة غير لائقة.
		4.4.12	فهم أنه ينبغي على الطلاب بناء علاقات محترمة على الإنترنت مع بعضهم البعض
		4.4.13	فهم أن الرسائل غير اللائقة التي ترسل من الطلاب الذين هم دون 18 عاما تعتبر جريمة جنائية.
	4.5 التطرف على الإنترنت	4.5.1	تحديد ما يجب معرفته التطرف على الإنترنت.
		4.5.2	فهم دور الإنترنت ووسائل التواصل الاجتماعي في توفير فرصة للتطرف الذاتي.
		4.5.3	التعرف على خصائص الطالب الضعيف والمؤشرات العامة للضعف التي تنطبق على التطرف.
		4.5.4	فهم كيفية منع الطلاب من الوقوع في براثن الإرهاب.
	4.6 الاستضعاف والمظلومية	4.6.1	تعريف مصطلحي الاستضعاف والمظلومية وفهم من هم عرضة للخطر على الإنترنت.
		4.6.2	فهم كيفية تجنب الوقوع ضحية للرسائل المزعجة و phishing وكيفية الحماية باستخدام منهجية التوقف والتفكير والاتصال.
		4.6.3	فهم أنه يجب على الطلاب عدم المجازفة بالاتصال بالإنترنت دون اتخاذ بعض الاحتياطات الأساسية ضد البرامج الضارة وبرامج البوتات.
		4.6.4	فهم الإجراء الذي يجب اتخاذه في حال تعرض الطالب لسرقة الهوية أو الاحتيال أو الجرائم الإلكترونية.
		4.6.5	فهم كيف يمكن للطلاب حماية مواردهم الرئيسية، مثل أجهزة الكمبيوتر والأجهزة اللوحية وأجهزة Ipad وما إلى ذلك

الموضوع	المهارة	رقم المرجع	نقاط الموضوع
5 إدارة سلامة الطالب على الإنترنت	4.7 التصدي لمخاطر "البث المباشر"	4.7.1	فهم المقصود بالبث المباشر عبر الإنترنت.
		4.7.2	شرح فرص ومخاطر البث المباشر عند مشاركة المحتوى على الإنترنت.
		5.1.1	فهم أن الاستماع الفعال يمكن أن يكون أداة قوية لتحسين التواصل وبناء علاقة إيجابية مع الطلاب.
		5.1.2	شرح مزايا استخدام الاستماع الفعال.
	5.1 الاستماع الفعال	5.1.3	فهم كيفية تحسين مهارات الاستماع الفعال.
		5.1.4	إدراك أن استراتيجية حل المشاكل هي مهارة حياتية هامة للمساعدة في حل مشاكل الطلاب.
		5.2.1	فهم كيف تساعد الثقة الطلاب على تصفح الإنترنت بأمان واتخاذ قرارات
		5.2.2	فهم كيفية بناء الثقة والمرونة لدى الطلاب من خلال اتباع إرشادات خاصة
		5.2.3	فهم الإجراء الذي يجب اتخاذه في حالة افتقار الطالب لثقته أو رفض تجربة بدائل جديدة.
	5.3 الحالة المزاجية للطلاب: تقلبات مرحلة المراهقة	5.3.1	فهم الحالة المزاجية المتغيرة عند الطلاب.
		5.3.2	التعرف على الدوافع المحفزة للطلاب مثل الدوافع الجسدية والدوافع العاطفية.
		5.3.3	فهم دور المعلم عند التعامل مع مشاعر الطلاب. تعلم معلومات جديدة للتعامل مع قلق الطلاب و/أو المشاعر الصعبة في المدرسة التي يمكن أن تؤثر على مستوى أدائه.
		5.4.1	التعرف على أهمية المواطنة الرقمية في الحفاظ على مسؤولية الطلاب وسلامتهم على الإنترنت.
	5.4 المواطنة الرقمية	5.4.2	تحديد الطرق التي يمكن من خلالها أن نكون مواطنين مسؤولين رقمياً، مثل الاحترام على الإنترنت وحماية سمعة الطلاب الآخرين. كن متشككاً وغير ساذج.
		5.5.1	تعريف مصطلح المرونة الرقمية. فهم معنى المرونة الرقمية.
		5.5.2	فهم أهمية المرونة الرقمية.
		5.5.3	فهم دور القيم والمواقف الشخصية في بناء المرونة.
6 تدابير وقائية لحماية الطلاب على الإنترنت	6.1 خصوصية الطالب والمراقبة والثقة	5.5.4	فهم أن المهارات الاجتماعية تشكل لبنة بناء هامة من أجل المرونة.
		5.5.5	تحديد عادات التفكير الإيجابية من أجل المرونة لمساعدة الطلاب على الاحتفاظ بالأشياء في منظورها الصحيح من خلال التركيز على الحقائق والحياة الواقعية.
		5.5.6	التعرف على كيفية تطوير المرونة الرقمية لدى الطالب لمساعدته في أن يصبح عميلاً فعالاً في حمايته وسلامته.
		6.1.1	فهم ما يشكل خصوصية الطالب على الإنترنت.
	6.2 الحفاظ على سلامة الطلاب على الإنترنت	6.1.2	فهم ما يجب أن تتضمنه سياسة مراقبة الطلاب في المدرسة.
		6.1.3	فهم مدى أهمية مراقبة نشاط الطالب على الإنترنت في المدرسة والمنزل
		6.1.4	إدراك أن استخدام تطبيقات المراقبة قد يكون له تأثيرات سلبية على ثقة الطالب
		6.1.5	شرح كيفية التعامل مع الطلاب في حالة انتهاك الثقة على الإنترنت أو إساءة استخدام الخصوصية على الإنترنت.
	6.2 الحفاظ على سلامة الطلاب على الإنترنت	6.2.1	فهم كيفية تحديد وإدارة سلامة الطلاب على الإنترنت لحمايتهم. التعرف على العلامات التي تدل على احتمال تعرض الطالب للإساءة على الإنترنت.
		6.2.2	فهم كيفية مساعدة الطلاب في تحديد وإدارة سلامتهم على الإنترنت.

الموضوع	المهارة	رقم المرجع	نقاط الموضوع
		6.2.3	فهم أهمية الاتصال المفتوح مع الطلاب فيما يتعلق بالوسائط الرقمية واستخدام الإنترنت والتجارب السيئة على الإنترنت. فهم كيفية اكتشاف عمليات الاحتيال والخداع على الإنترنت باستخدام Hoax-Slayer.
		6.2.4	فهم كيفية منع الطلاب من الوقوع ضحية لجرائم الإنترنت، والتنزيل غير المتعمد للفيروسات وكيفية التصفح بأمان.
	6.3 تعلم السلوك الآمن والمسؤول على الإنترنت	6.3.1	فهم كيف يمكن للطلاب إدارة سلامتهم على الإنترنت بأنفسهم.
		6.3.2	التعرف على كيفية مراجعة التطبيقات والمحتوى للتأكد من ملاءمتها من خلال مشاركة الخبرات على الإنترنت مع الطلاب
		6.3.3	فهم أن الحوار المستمر مطلوب لإبقاء قنوات الاتصال مفتوحة مع الطلاب.
		6.3.4	تحديد المخاطر التي يواجهها الطلاب فيما يتعلق بالخصوصية والمعلومات الشخصية.
		6.3.5	فهم كيفية التحدث بشكل مناسب عند التحدث إلى الطلاب عن آداب السلوك على الإنترنت والاستخدام السليم لمفردات اللغة.
		6.3.6	التعرف على دور الوالدين فيما يتعلق بالمخاطر التي قد يواجهها أطفالهم ومساعدتهم على تحديد استراتيجيات مناسبة لحماية أطفالهم في المنزل.
	6.4 مناقشة السلامة على الإنترنت مع الطلاب	6.4.1	التعرف على العلامات التي تدل على أن الطالب يتعرض لمخاطر سلوكية غير المرغوب بها على الإنترنت
		6.4.2	فهم أنه يمكن استخدام تطبيقات الرقابة الأبوية على الإنترنت في المدرسة أيضاً لحماية الطلاب.
		6.4.3	فهم أدوات وعادات الإنترنت الجيدة التي يمكن الاعتماد عليها لحماية الطلاب.
7 دليل موارد الصف لإشراك الطلاب في الأمن الرقمي	7.1 موارد التطوير المهني في غرفة الصف	7.1.1	تحديد مراحل التقنية المتكاملة، والتي تتضمن الاستبدال والتعزيز والتعديل وإعادة التحديد.
		7.1.2	فهم أنه يمكن تشجيع الطلاب على ممارسة الأمن الرقمي من خلال الأنشطة المدرسية، مثل معسكر تدريب أو مسابقة.
		7.1.3	التعرف على كيفية دمج مفاهيم الأمن الرقمي في الصف.
		7.1.4	يمارس الطلاب الاستراتيجيات الآمنة لإطار عمل C3
8 سياسة الأمن الرقمي	8.1 إعداد دليل سياسات	8.1.1	فهم السياسات التي يجب تغطيتها لحماية أنشطة الطلاب على الإنترنت.
		8.1.2	فهم الموارد المطلوبة لتطبيق سياسة المدرسة على الإنترنت والحفاظ عليها
		8.1.3	فهم أنواع المشاكل التي يجب إبلاغ المدرسة بها
		8.1.4	فهم كيفية معالجة استجابات الحوادث المرتبطة بالأجهزة الرقمية للطلاب.
9 أخلاقيات الإنترنت	9.1 ما هي المشكلات الأخلاقية المهمة في الأمن الرقمي؟	9.1.1	فهم النظريات الأخلاقية المعروفة، مثل المبادئ الأخلاقية والسلوكية.
		9.1.2	فهم أهمية المشاكل الأخلاقية عندما يتعلق الأمر بإيذاء الطلاب أو مساعدتهم.
		9.1.3	تحديد كيف يقوم المعلمين بتطبيق الميثاق الأخلاقي
		9.1.4	فهم كيفية مراقبة الطلاب بفاعلية دون انتهاك خصوصية الطلاب.
		9.1.5	فهم كيف ينبغي على المعلمين مراقبة أنشطة الطلاب.
	9.2 المفاهيم الأخلاقية: اتصالات الشبكة في الأمن الرقمي؟	9.2.1	تحديد الآداب المتعلقة بإرسال الرسائل.
		9.2.2	التعرف على آداب التفاعل الفعال على الإنترنت.
		9.2.3	التعرف على كيفية التعامل مع التنمر الإلكتروني بطريقة أخلاقية.

الموضوع	المهارة	رقم المرجع	نقاط الموضوع
10 قوانين الإنترنت	10.1 الوعي والإرشادات	9.2.4	التعرف على علامات إدمان الإنترنت وكيفية التعامل معها .
		9.2.5	فهم القواعد التي يجب اتباعها مع المحتوى غير اللائق عند استخدام التقنية الرقمية بما في ذلك خيار تصفية المحتوى وإرسال الرسائل.
		10.1.1	فهم كيفية التمييز بين الجريمة والالتزامات الأخلاقية. فهم قوانين الإنترنت المحددة التي قد ينتهكها الطلاب.
		10.1.2	التعرف على كيفية حماية الملكية الفكرية بما في ذلك الأسرار التجارية والعلامات التجارية وحقوق النشر وبراءات الاختراع.
		10.1.3	فهم قوانين الخصوصية والسرية التي يتم تطبيقها عند نشر الصور
		10.1.4	فهم الآثار القانونية لتحميل وتنزيل الوسائط.
		10.1.5	التعرف على التحديات القانونية عند استخدام وسائل التواصل الاجتماعي.