

**السلامة على الإنترنت**  
منهج إصدار ٢





## أهداف المقرر

يزود مقرر **السلامة على الإنترنت** المرشحين بالمهارات والمعارف المطلوبة للتعامل الآمن مع أجهزة الكمبيوتر والأجهزة المحمولة لتفادي مخاطر الإنترنت، حيث سيدرك المرشحون أهمية حماية المعلومات الشخصية على أجهزة الكمبيوتر والأجهزة المحمولة وسيتعرفون على التهديدات التي تشكلها عمليات الإجرام والاحتيال على الإنترنت.

كما سيتعرف المرشحون على التهديدات التي تشكلها الفيروسات، وسيدركون أهمية استخدام برامج مكافحة الفيروسات وجدوان الحماية، وسيتعرفون أيضاً على إجراءات النسخ الاحتياطي واستخدام كلمات المرور الجيدة وكيفية تنقية الرسائل غير المرغوب فيها من البريد الإلكتروني جنباً إلى جنب مع إدراك أهمية فحص مرفقات البريد الإلكتروني قبل فتحها.

وسيتعرف المرشحون أيضاً على المعلومات الواردة في الأجهزة الذكية وكيفية تبادلها عبر الإنترنت، وكيفية تعيين ميزات الأمان المناسبة للأجهزة الذكية للوقاية من التهديدات الأمنية ومنع الوصول غير المصرح به إلى الجهاز والبيانات التي يحتوي عليها.

وسيتعرف المرشحون بجانب ذلك على المخاطر الكامنة في الاستخدام اليومي للإنترنت، وكيفية حماية أنفسهم عند التسوق عبر الإنترنت، وكذلك الآثار المترتبة على وضع المعلومات الشخصية على مواقع التواصل الاجتماعي، بالإضافة إلى الأمور المتعلقة بالخصوصية، والأجهزة التي يمكن استخدامها لتبادل المعلومات جنباً إلى جنب مع كيفية إمكان استخدام ميزات الصور والفيديوهات لتسجيل ومشاركة المعلومات غير الآمنة.

هذا وسيتعرف المرشحون على بعض المخاطر المرتبطة بشبكات التواصل الاجتماعي التي من بينها: المحتوى غير اللائق وقضايا التحقق من السن والوصول إلى الملفات التعريفية واحتمالية التعرض للمعتدين، فضلاً عن التهديدات التي تشكلها هجمات الهندسة الاجتماعية، والتهديدات على الإنترنت التي يتعرض لها الأطفال عن طريق استخدام هويات زائفة على وسائل التواصل الاجتماعي.

أهمية عدم تداول المواد التي قد تضر الآخرين، ومعرفة كيفية رفض أو منع الغرباء أو الاتصالات غير المرغوب فيها، واستخدام كاميرا الويب مع الأشخاص الذين تعرفهم فقط، ومعاملة الآخرين عبر الإنترنت بالاحترام.

كما سيتعلم المرشحون كيفية إعداد ضوابط المراقبة الأبوية لحماية أنشطة أطفالهم على الإنترنت، واختيار برامج التنقية والمراقبة واستخدامها، وذلك جنباً إلى جنب مع إدراك مفهوم إدمان الإنترنت، وكيفية التعرف على أعراض هذه المشكلة والتعامل معها، فضلاً عن معرفة وفهم التسلط عبر الإنترنت وفهم الوسائل التي يمكن أن يحدث من خلالها، وكذلك التعرف على علامات التحذير من التسلط عبر الإنترنت ومعرفة كيفية مواجهته، بالإضافة إلى معرفة أسباب دعوة المؤسسات إلى إرساء سياسات الاستخدام المقبول وتبنيها، جنباً إلى جنب مع التعرف على عناصر السياسات الفعالة.

موضوع المهمة	المرجع	مجموعة المهارات	الفئة
إدراك أهمية حماية المعلومات الشخصية الموجودة على جهاز الكمبيوتر الخاص بك.	١-١-١-٢	١-١-٢ الهوية	١-٢ الحماية
التعرف على التهديدات التي تشكلها عمليات الإجرام والاحتيال على الإنترنت.	٢-١-١-٢		
تجنب عمليات الاحتيال والخداع مثل: التصيد الاحتيالي وتزوير العناوين والقرصنة.	٣-١-١-٢		
تجنب عمليات الاحتيال والخداع مثل: التصيد الاحتيالي وتزوير العناوين والقرصنة.	٤-١-١-٢		
معرفة آليات وضع ممارسات جيدة لتعيين كلمات مرور من حيث طول كلمة المرور والرموز الأبجدية الرقمية وتكرار التغيير.	١-٢-١-٢	٢-١-٢ المصادقة	



موضوع المهمة	المرجع	مجموعة المهارات	الفئة
معرفة آليات وضع ممارسات جيدة لتعيين كلمات مرور من حيث الطول والرموز الأبجدية الرقمية وتكرار التغيير.	٢-٢-١-٢		
فهم معنى المصادقة الثنائية: الرموز، والبطاقات الذكية، والمقاييس الحيوية.	٣-٢-١-٢		
استيعاب الغرض من برامج مكافحة الفيروسات.	٢-٣-٢-١	٣-٢-١ مكافحة الفيروسات	
استيعاب ضرورة المواظبة على تحديث برنامج مكافحة الفيروسات.	٣-٣-٢-١		
التعرف على عمل جدار الحماية ومدى أهميته.	٤-٣-٢-١		
استيعاب مصطلح برامج التجسس والمخاطر المرتبطة بها.	١-٤-٢-١	٣-٢-١ مكافحة التجسس	
معرفة كيفية تشغيل برامج مكافحة التجسس وكيفية إزالة برامج التجسس من الكمبيوتر.	٢-٤-٢-١		
التعرف على علامات التحذير التي تشير إلى احتمالية وجود برنامج تجسس على جهازك.	٣-٤-٢-١		
فهم معنى النسخ الاحتياطي وأسباب أهميته.	١-١-٢-٢	١-٢-٢ النسخ الاحتياطي	٢-٢ التأمين
التعرف على أجهزة النسخ الاحتياطي الشائعة: الأقراص المضغوطة وأقراص DVD ومشغلات USB ومشغلات الأقراص الصلبة الخارجية، ومعرفة السعات المختلفة.	٢-١-٢-٢		
استيعاب مفهوم النسخ الاحتياطي السحابي.	٣-١-٢-٢		
استخدام خصائص النسخ الاحتياطي على جهاز الكمبيوتر الخاص بك، وفهم معنى "استعادة" النسخة الاحتياطية.	٤-١-٢-٢		
استيعاب مفهوم رسائل البريد الإلكتروني غير المرغوب فيها / المزعجة وضرورة تنقية البريد الإلكتروني.	١-٢-٢-٢	٢-٢-٢ البريد الإلكتروني	
تفعيل عامل تصفية الرسائل المزعجة في البريد الإلكتروني.	٢-٢-٢-٢		
ضبط إعدادات تصفية الرسائل المزعجة.	٣-٢-٢-٢		
فهم ماهية الشبكات اللاسلكية أو شبكات الواي فاي.	١-٣-٢-٢	٣-٢-٢ الشبكات اللاسلكية	

موضوع المهمة	المرجع	مجموعة المهارات	الفئة
التعرف على المزايا والمخاطر المرتبطة باستخدام نقاط اتصال العامة Wi-Fi.	٢-٣-٢-٢		
التعرف على ميزات الحماية الخاصة باستخدام أحدث البروتوكولات اللاسلكية.	٣-٣-٢-٢		
التعرف على اعتبارات الأمن المادي عند استخدام الكمبيوتر المحمول والأجهزة اللوحية.	١-٤-٢-٢	٤-٢-٢ مادي	
معرفة كيفية تقليل المخاطر المرتبطة بسرقة الجهاز أو فقدانه: إبقاء الجهاز نصب العينين، واستخدام سلك الحماية (إذا كان ذلك مناسباً)، والتأمين بكلمة مرور، وتدوين الرقم التسلسلي، واستخدام الرسم بالأقلام السرية.	٢-٤-٢-٢		
التعرف على قضايا الحماية فيما يتعلق بالتخلص من أجهزة الكمبيوتر، وأهمية إزالة البيانات قبل التخلص منها.	٣-٤-٢-٢		
التعرف على البيانات التي يحويها جهازك ويشاركها على الإنترنت وكيف يمكن أن يساء استخدامها.	١-٥-٢-٢	٥-٢-٢ الأجهزة الذكية	
التعرف على مميزات الأمان الأساسية: حماية الجهاز بكلمة المرور، إعداد خدمة القفل التلقائي، تثبيت برنامج حماية، تثبيت تحديثات نظام التشغيل، تتبع الهاتف المحمول.	٢-٥-٢-٢		
معرفة كيف أن استخدام التشفير على هاتفك الذكي يمكن أن يساعد على منع سرقة البيانات.	٣-٥-٢-٢		
التعرف على المسائل الأمنية المتعلقة بالتطبيقات، تنزيل التطبيقات من المصادر المعتمدة فقط، والتحقق من صلاحيات التطبيقات.	٤-٥-٢-٢		
التعرف على الفيروسات الموجودة على أنظمة تشغيل الهواتف المحمولة والبرامج الخبيثة للهواتف المحمولة.	٥-٥-٢-٢		
التعرف على التهديدات الأمنية القادمة عبر البريد الإلكتروني أو الرسائل النصية غير المرغوب فيها، والتعرف على أعراض الإصابة بالبرامج الضارة: رسوم بيانات غير عادية على الفاتورة، تغييرات غير مفهومة في واجهة المستخدم.	٦-٥-٢-٢		

موضوع المهمة	المرجع	مجموعة المهارات	الفئة
معرفة كيفية إيقاف وظائف "الواي فاي" و"البلوتوث" التلقائية لمنع الوصول غير المصرح به إلى الجهاز أو البيانات الخاصة بك.	٧-٥-٢-٢		
معرفة كيفية حذف جميع المعلومات الشخصية عند التخلص من الجهاز.	٨-٥-٢-٢		
معرفة كيفية تمكين إعدادات تحديد المواقع وتعطيلها، وفهم مزايا وعيوب تمكين إعدادات تحديد المواقع.	٩-٥-٢-٢		
تبادل رقم هاتفك المحمول مع من تعرفه وتثق به فقط، والاحتفاظ بسجل رقم IMEI الخاص بك في حالة فقدان الهاتف أو سرقة.	١٠-٥-٢-٢		
كيفية تطبيق التصفيه على الإنترنت لحجب المحتوى غير اللائق.	١١-٥-٢-٢		
التعرف على مخاطر الاستخدام اليومي للإنترنت: البريد الإلكتروني، تصفح الإنترنت، الأعمال المصرفية عبر الإنترنت، التسوق عبر الإنترنت، شبكات التواصل الاجتماعي وغيرها.	١-١-٣-٢	١-٣-٢ مخاطر الإنترنت	٣-٢ توكي الحذر
التعرف على مدى إنتشار المواد غير اللائقة على الإنترنت.	٢-١-٣-٢		
الحذر من المخاطر الشائعة: التعرف على مخاطر الطلبات الواردة عبر البريد الإلكتروني المشتبه بها ومواقع الويب المحتمل أن تكون ضارة.	٣-١-٣-٢		
التعرف على كيفية توفير الحماية الكافية لنفسك قبل التسوق عبر الإنترنت: استخدام الإصدار الأحدث من المتصفحات، والتأكد من تحديث برنامج مكافحة الفيروسات، وما إلى ذلك.	١-٢-٣-٢	٢-٣-٢ التسوق عبر الإنترنت	
التعرف على كيفية تحديد المواقع الآمنة: ظهور أيقونة القفل على شريط حالة المتصفح، وظهور حرف "s" بعد http في عنوان URL.	٢-٢-٣-٢		
التعرف على سياسات الخصوصية.	٣-٢-٣-٢		



موضوع المهمة	المرجع	مجموعة المهارات	الفئة
توخ الحذر من المعلومات التي يتم تجميعها لإتمام المعاملات وتحديد ما إذا كانت ملائمة أم لا.	٤-٢-٣-٢		
الانتباه إلى خيارات الدفع الآمنة: بطاقات الائتمان، وبطاقات السحب، وغيرها.	١-٣-٣-٢	٣-٣-٢ الدفع عبر الإنترنت	
التعرف على الوقت المناسب لاستخدام أدوات الإكمال التلقائي وإيقاف تشغيلها.	٢-٣-٣-٢		
التعرف على وسائل الأمان المختلفة الخاصة بعملية الدفع: استخدام مانع العناصر المنبثقة، إيقاف تشغيل أدوات الإكمال التلقائي، أمان المتصفح، إعدادات التصفية.	٣-٣-٣-٢		
استيعاب مفهوم الهوية عبر الإنترنت وما تعنيه شبكات التواصل الاجتماعي.	١-١-٤-٢	١-٤-٢ الهوية الشخصية	٤-٢ فكر أولاً
معرفة الآثار المترتبة على وضع المعلومات الشخصية على الإنترنت.	٢-١-٤-٢		
التفكير في من يمكنه الدخول إلى بياناتك الشخصية: الأصدقاء، زملاء العمل، أصحاب العمل، المجرمون، المعتدون.	٣-١-٤-٢		
التعرف على خيارات الخصوصية بشبكات التواصل الاجتماعي وسبب أهميتها.	٤-١-٤-٢		
التعرف على أنواع الأجهزة التي يمكن استخدامها في تبادل المعلومات: الهواتف المحمولة، الهواتف الذكية، مشغلات MP3، أجهزة الآي بود، الأجهزة اللوحية، إلخ.	١-٢-٤-٢	٢-٤-٢ دوات المشاركة	
الانتباه إلى إمكانية استخدام خصائص الصور والفيديو لتسجيل ونشر محتوى غير لائق على الإنترنت.	٢-٢-٤-٢		
توخي الحذر عند نشر الصور أو مقاطع الفيديو على الإنترنت من خلال هاتفك المحمول، وطلب إذن الآخرين قبل نشر الصور أو مقاطع الفيديو الخاصة بهم من خلال هاتفك المحمول.	٣-٢-٤-٢		
التعرف على مختلف مواقع شبكات التواصل الاجتماعي التي يستخدمها الشباب مثل: فيس بوك وغوغل+، وتويتر وموقع هايه وماي سبيس.	١-٣-٤-٢	٣-٤-٢ شبكات التواصل الاجتماعي	



موضوع المهمة	المرجع	مجموعة المهارات	الفئة
التعرّف على طريقة إنشاء ملف شخصي على شبكات التواصل الاجتماعي وكيفية ضبط ملفك الشخصي للعرض الشخصي أو العام.	٢-٣-٤-٢		
استيعاب فكرة إمكانية رؤية أي شخص لملفك الشخصي على الإنترنت والبحث عنك باستخدام بعض المعايير والوصول إلى معلوماتك الشخصية.	٣-٣-٤-٢		
التعرّف على بعض مخاطر استخدام شبكات التواصل الاجتماعي: المحتوى غير اللائق، ومسائل التحقق من العمر، والدخول إلى الملفات الشخصية، واحتمالية وجود مستغلين.	٤-٣-٤-٢		
إدراك أن البريد الإلكتروني غير المرغوب والتصيد الاحتمالي منتشران أيضا على مواقع شبكة التواصل الاجتماعي.	١-٤-٤-٢	٤-٤-٢ البريد الإلكتروني غير المرغوب فيه والتصيد الاحتمالي على منصات التواصل الاجتماعي	
التعرف على الروابط المشبوهة للإعلانات على الإنترنت وتحديثات الحالة والتغريدات والمشاركات الأخرى.	٢-٤-٤-٢		
فهم مصطلح "الهندسة الاجتماعية" والاحتياط من التهديدات التي تشكلها هجمات الهندسة الاجتماعية.	٣-٤-٤-٢		
إدراك سهولة إنشاء ملف شخصي على مواقع شبكات التواصل الاجتماعي، وإمكانية استخدام المجرمين ذلك كفرصة لانتحال صفة شخص آخر.	٤-٤-٤-٢		
التعرف على التهديدات التي يتعرض لها الأطفال عبر الانترنت عن طريق استخدام هويات زائفة: الاستمالة، واستغلال الأطفال.	١-٥-٤-٢	١-٥-١ الوعي	
تعرف على التهديدات العبر الانترنت التي يتعرض لها الكبار عن طريق استخدام هويات زائفة.	٢-٥-٤-٢		
التعرف على خاصية المراسلة الفورية وغرف الدردشة.	١-١-٥-٢	١-٥-٢ المراسلة الفورية/ غرف الدردشة	٥-٢ السلوك الافتراضي
تعلم كيفية إنشاء ملف شخصي لبرامج المراسلة الفورية.	٢-١-٥-٢		

موضوع المهمة	المرجع	مجموعة المهارات	الفئة
ضبط الخيارات للسماح لقائمة الأصدقاء فقط بالتحدث إليك، وحجب الأشخاص الذين لا ترغب في التحدث إليهم.	٣-١-٥-٢		
معرفة آليات تعطيل كاميرا الويب.	٤-١-٥-٢		
التعرف على إمكانية مشاركة مقاطع الفيديو على الإنترنت من خلال: يوتيوب، ماي سبيس تي في، الخ	١-٢-٥-٢	٢-٥-٢ مقاطع الفيديو، المدونات	
استيعاب مفهوم المدونات والمدونات المصغرة وكيفية دمجها مع شبكات التواصل الاجتماعي.	٢-٢-٥-٢		
التعرف على المخاطر المصاحبة لتسريب المعلومات الشخصية أو القذف أو النميمة من خلال المدونات.	٣-٢-٥-٢		
استيعاب آليات عمل مواقع مشاركة الملفات واحتمالية الإصابة بالفيروسات والبرامج الضارة أثناء استخدام مواقع مشاركة الملفات.	٤-٢-٥-٢		
الاحتراس من ألعاب تقمص الأدوار الموجودة على الإنترنت وما يتعلق بها من مخاطر مثل: اللاعبون المجهولون، والوصول لمستوى الإدمان.	١-٣-٥-٢	٣-٥-٢ الألعاب على الإنترنت	
تجنب تداول الرسائل أو الصور أو غيرها من المواد المسيئة، ومشاركة الصور مع الأشخاص الذين تعرفهم وتثق بهم فقط.	١-٤-٥-٢	٤-٥-٢ تحمل المسؤولية	
معرفة كيفية رفض أو منع الغرباء والاتصالات غير المرغوب فيها، والحذر من التخطيط لمقابلة أشخاص لا تعرفهم، حتى لو كانوا أصدقاء لك على الإنترنت.	٢-٤-٥-٢		
استخدام كاميرا ويب مع من تعرفهم فقط، وفصلها أو تعطيلها عند عدم استخدامها.	٣-٤-٥-٢		
إدراك أن تنزيل الموسيقى والأفلام والصور وبرامج الكمبيوتر والألعاب من على الإنترنت قد يكون مخالفا للقانون ما لم ينص على ذلك صراحة على الموقع المستخدم.	٤-٤-٥-٢		
معاملة الآخرين على الإنترنت كما تحب أن يعاملوك به.	٥-٤-٥-٢		

موضوع المهمة	المرجع	مجموعة المهارات	الفئة
التعلم سويًا ومناقشة موضوع استخدام الكمبيوتر مع أصدقائك وأسرتك.	١-١-٦-٢	١-٦-٢ المناقشة	٦-٢ التعلم سويًا
قبول حقيقة أن ترك أجهزة الكمبيوتر المنزلية في مواقع مركزية مفتوحة هو الإجراء الأفضل.	٢-١-٦-٢		
الإلمام ببرامج التصفية والمراقبة من أجل تصفية الصور الإباحية وأنشطة التسجيل عبر الإنترنت وضبط موقتات الإنترنت وحظر إرسال المعلومات الشخصية عبر البريد الإلكتروني أو نشرها.	٣-١-٦-٢		
إدراك أن برامج المراقبة الأبوية متوفرة في مجموعة من أجهزة الوسائط مثل: التلفزيون الرقمي، ألعاب الفيديو والكمبيوتر والهواتف المحمولة وأجهزة iPods والأجهزة اللوحية وبرامج الكمبيوتر	١-٢-٦-٢	٢-٦-٢ المراقبة	
ضبط برامج المراقبة الأبوية على برامج التشغيل.	٢-٢-٦-٢		
كيفية تثبيت بعض برامج المراقبة الأبوية أو تنزيلها: <a href="http://www-theparentalcontrolbar-org">www-theparentalcontrolbar-org</a>	٣-٢-٦-٢		
التعرف على أهمية إنشاء حسابات مستخدم متعددة بامتيازات وصول مختلفة لكل حساب.	٤-٢-٦-٢		
التعرف على أسباب إنشاء حساب إلكتروني للطفل وتوجيه الرسائل الواردة بصندوق الوارد ببرنامج المراقبة الأبوية لاستعراضها.	٥-٢-٦-٢		
التعرف على المعايير التي يجب مراعاتها عند اختيار برنامج لتصفية المحتوى خاص بالآباء، كيف يطبق البرنامج على الأنواع المختلفة من الأجهزة، مثل الهواتف الذكية أو أنظمة الألعاب؟	٦-٢-٦-٢		
الاطلاع على الطريقة التي يمكن للشباب من خلالها إخفاء الأنشطة التي يمارسونها عبر الإنترنت عن الآباء.	٧-٢-٦-٢		
التعرف على الطرق التي تمنع الشباب من حجب أنشطتهم عبر الإنترنت.	٨-٢-٦-٢		

موضوع المهمة	المرجع	مجموعة المهارات	الفئة
التعرف على أن برامج التصفية ليست بديلاً عن إشراف الوالدين الصحيح والنقاش المفتوح مع الأطفال والمراهقين.	٩-٢-٦-٢		
التعرف على كيفية إنشاء اتفاقية مستخدم إنترنت للآباء والأطفال.	١٠-٢-٦-٢		
إدراك كيف أن استخدام الإنترنت يمكن أن يتداخل مع الحياة اليومية والعمل والعلاقات.	١-٣-٦-٢	٣-٦-٢ إدمان الإنترنت	
التعرف على مفهوم اضطرابات إدمان الإنترنت والأنواع المختلفة لمشاكل الإدمان: المحتوى غير اللائق، وغرف الدردشة، وألعاب الإنترنت، وتصفح الإنترنت القهري.	٢-٣-٦-٢		
التعرف على بعض أعراض اضطرابات إدمان الإنترنت: فقدان مسار الوقت على الإنترنت، الانعزال عن الأسرة والأصدقاء، الدفاع عن استخدام الإنترنت، صعوبة استكمال المهام الأخرى، اضطرابات أثناء النوم.	٣-٣-٦-٢		
التعرف على كيفية مساعدة الطفل في علاج إدمان الإنترنت: تشجيع الاهتمامات والأنشطة الاجتماعية الأخرى، مراقبة استخدام الحاسوب ووضع حدود واضحة، استخدام تطبيقات للحد من استخدام الطفل للهاتف الذكي، مناقشة القضايا الأساسية مع الطفل، الحصول على مساعدة مهنية.	٤-٣-٦-٢		
اختبار إدمان الإنترنت	٥-٣-٦-٢		
استيعاب معنى مصطلح "آداب التعامل على الإنترنت".	١-١-٧-٢	١-٧-٢ التواصل	٧-٢ السلوك الافتراضي
إدراك مفهوم "لا تراجع" فور نشر معلومات.	٢-١-٧-٢		
الهدف من اختيار إسم مستخدم "ذكي" على الإنترنت لا يفصح إلا عن جزء قليل جداً من المعلومات الشخصية.	٣-١-٧-٢		
التعرف على سبب أهمية حماية المعلومات الشخصية والحفاظ على الخصوصية.	٤-١-٧-٢		
اتخاذ الحيلة من إضافة أشخاص لا تعرفهم إلى قائمة الأصدقاء/الزملاء لتجنب المخاطر.	٥-١-٧-٢		

موضوع المهمة	المرجع	مجموعة المهارات	الفئة
التعرف على مصطلح "التسلط عبر الإنترنت".	١-٢-٧-٢	٢-٧-٢ المضايقات الإلكترونية	
التعرف على الوسائل التي يتم من خلالها التسلط عبر الإنترنت.	٢-٢-٧-٢		
التعرف على مدى سرعة انتشار المعلومات/ الصور وما هي التأثيرات المترتبة على التسلط عبر الإنترنت.	٣-٢-٧-٢		
التعرف على عواقب التسلط عبر الإنترنت ودوافعه التي منها: إخفاء الهوية، حيث يشعر المتسلط بأنه قادر على "الهروب بفعلته"، والتعرف على أن التسلط عبر الإنترنت يمكن أن يكون عملية ذات اتجاهين.	٤-٢-٧-٢		
التعرف على علامات التحذير من التسلط عبر الإنترنت ومعرفة كيف يمكن للأطفال مواجهته:	٥-٢-٧-٢		
<ul style="list-style-type: none"> <li>• الشعور بالحزن أو القلق أو تغيير المزاج</li> <li>• التغيب من المدرسة</li> <li>• الانسحاب من أو إظهار نقاط الاهتمام في الأنشطة الاجتماعية</li> <li>• الحصول على درجات منخفضة أو ضعف الأداء الأكاديمي</li> <li>• الشعور بالقلق بعد استخدام الحاسب الآلي أو الاتصال بالإنترنت</li> </ul>			
تعلم كيف يمكن مواجهة التسلط عبر الإنترنت وتسجيله وإبلاغ السلطات المختصة عما به من مخاوف.	٦-٢-٧-٢		
ماذا لو كان طفلك متسلطاً؟ نصائح للآباء (والمعلمين) بشأن كيفية التعامل مع الأطفال المتسلطين على الآخرين عبر الإنترنت.	٧-٢-٧-٢		
التعليقات غير الملائمة في الرسائل، ورسائل البريد الإلكتروني أو المنتديات العامة ومواقع التواصل الاجتماعي والنصوص غير المناسبة والملاحقة الإلكترونية، التمييز بين الملاحقة الإلكترونية والهندسة الاجتماعية.	٨-٢-٧-٢		
معرفة سياسة الاستخدام المقبول وأهميتها في المنظمات.	١-١-٨-٢	١-٨-٢ الاستخدام	٨-٢ لسياسة المتبعة

موضوع المهمة	المرجع	مجموعة المهارات	الفئة
معرفة محتويات سياسة الاستخدام المقبول السليمة: توعية المستخدمين، والحد من المخاطر، ودعم آداب استخدام الإنترنت والسلوكيات الاجتماعية والأخلاقية الملائمة، وحماية المستخدمين قليلي الخبرة، وحماية الهوية الشخصية.	٢-١-٨-٢		
فهم سياسات تعديل عامل تشغيل الهاتف المحمول مع الأخذ في الاعتبار الوصول إلى غرف الدردشة أو الألعاب والتحكم في رسائل البريد الإلكتروني غير المرغوب فيها.	٣-١-٨-٢		
الدراية بقوانين حقوق الطبع والنشر وأثرها في حالة التنزيل غير القانوني من خلال خدمات مشاركة الملفات.	١-٢-٨-٢	٢-٨-٢ حقوق الطبع والنش	
إدراك عدم شرعية قرصنة الموسيقى والأفلام والبرامج وإدراك تأثيرات هذه الأعمال.	٢-٢-٨-٢		

### ملحق إلى كتيب الامان:

- ١- نصائح للوالدين فيما يتعلق بالأمان عبر الإنترنت.
- ٢- المبادئ التوجيهية لسياسة الأمان عبر الإنترنت للمدارس وطلب النصائح من المدرسين.
- ٣- نصائح لمستخدمي الإنترنت (المراهقين والآباء) فيما يتعلق بالأمان عبر الإنترنت.