تاريخ المراجعة: سنوياً
مسؤول المراجعة: رئيس قسم تكنولوجيا المعلومات، أخصائية المدرسة والمدير الأكاديمي

سياسة السلامة الالكترونية

الأسباب

تعد التقنيات الجديدة جزءًا لا يتجزأ من حياة البالغين والمراهقين والأطفال الصغار في مجتمع اليوم، سواء داخل المدرسة أو في حياتهم خارجها.

الإنترنت وغيرها من التقنيات الرقمية والمعلوماتية أدوات قوية تفتح فرصًا جديدة للجميع. يساعد الاتصال الإلكتروني المعلمين والطلاب على التعلم من بعضهم البعض. يمكن لهذه التقنيات أن تحفز المناقشة وتعزز الإبداع وتزيد من الوعي بالسياق لتعزيز التعلم الفعال. يحق للطلاب دائمًا الوصول الآمن إلى الإنترنت.

يجب التأكد من أن الطلاب يمكنهم استخدام الإنترنت وتقنيات الاتصالات ذات الصلة بشكل مناسب وآمن كجزء من الرعاية الأوسع الذي يلتزم به جميع العاملين في المدارس. ستساعد سياسة السلامة الإلكترونية الخاصة بنا على ضمان الاستخدام الآمن والمناسب. يحتاج تنفيذ هذه السياسة إلى إشراك جميع أصحاب المصلحة في تعليم الطفل من مديري المدارس والمحافظين إلى كبار القادة ومعلمي الفصل الدراسي وموظفي الدعم وأولياء الأمور وأعضاء المجتمع والطلاب أنفسهم.

يجب في مدرسة قطر العالمية أن يلتزم جميع مستخدمي الإنترنت بهذه السياسة بالإضافة إلى أي قوانين محلية ودولية تتعلق بحماية الطفل عبر الإنترنت، وحقوق الأسرة، والمطاردة أو التنمر الالكتروني والقرصنة.

الأهداف

الهدف من هذه السياسة هو توجيه الطلبة (وأولياء أمورهم / مقدمي الرعاية لهم) والموظفين والمستخدمين الآخرين لأنظمتنا ومعداتنا ليكونوا مستخدمين مسؤولين وأن يظلوا آمنين أثناء استخدام الإنترنت وتقنيات الاتصالات الأخرى للاستخدام التعليمي والشخصي والترفيهي.

يمكن أن يؤدي استخدام التكنولوجيا إلى تعريض الطلاب للخطر داخل المدرسة وخارجها. تتضمن بعض المخاطر التي قد يتعرضون لها ما يلي:

- الوصول إلى صور أو محتوى آخر غير قانوني أو ضار أو غير مناسب.
- الاتصال غير الملائم مع الآخرين، بما في ذلك الغرباء.
- التنمر الإلكتروني.
- فقدان و / أو تلف البيانات الشخصية.
- إمكانية الاستخدام المفرط، مما قد يؤثر على النمو الاجتماعي والعاطفي وتعلم الشاب.

يمكن أن يؤدي استخدام التكنولوجيا إلى تعريض الطلاب للخطر داخل المدرسة وخارجها. تعكس العديد من هذه المخاطر المواقف في العالم غير المتصل بالإنترنت ومن الضروري استخدام سياسة السلامة الإلكترونية هذه جنبًا إلى جنب مع سياسات المدرسة الأخرى (مثل سياسة الحماية).

كما هو الحال مع جميع المخاطر الأخرى، من المستحيل القضاء على هذه المخاطر تمامًا. لذلك من الضروري، من خلال توفير التعليم الجيد، بناء قدرة الطلاب على الصمود أمام المخاطر التي قد يتعرضون لها، بحيث يكون لديهم الثقة والمهارات اللازمة لمواجهة هذه المخاطر والتعامل معها.

تنطبق هذه السياسة على جميع أعضاء المجتمع المدرسي (بما في ذلك الموظفون والطلبة والمتطوعون وأولياء الأمور / مقدمو الرعاية والزوار) الذين يمكنهم الوصول إلى أنظمة تكنولوجيا المعلومات والاتصالات في المدرسة والمستخدمين لها، سواء داخل المدرسة أو خارجها.

تُستخدم هذه السياسة أيضًا لتنظيم سلوك الطلاب عندما يكونون خارج موقع المدرسة وتمكين أعضاء هيئة التدريس من فرض عقوبات تأديبية على السلوك غير اللائق. هذا وثيق الصلة بحوادث التسلط عبر الإنترنت أو غيرها من حوادث السلامة الإلكترونية التي تغطيها هذه السياسة، والتي قد تحدث خارج المدرسة، ولكنها مرتبطة بعضوية المدرسة.

تتعامل المدرسة مع مثل هذه الحوادث ضمن هذه السياسة والسلوك المرتبط بها وسياسات مكافحة التنمر، وستقوم، حيثما كان معروفًا، بإبلاغ أولياء الأمور / مقدمي الرعاية بحوادث السلوك غير الملائم للسلامة الإلكترونية التي تحدث داخل المدرسة أو خارجها.

الإجراءات

1. حماية البيانات والسلامة والخصوصية الشخصية:

1.1 حماية البيانات

يتم تسجيل البيانات الشخصية ومعالجتها ونقلها وإتاحتها وفقًا لقانون حماية البيانات لعام 1998 الذي ينص على أن البيانات الشخصية يجب أن تكون:

- معالجة عادلة وقانونية.
- تمت معالجتها لأغراض محدودة.
- كافية وذات صلة وغير مفرطة.
- دقيقة.
- لم يتم الاحتفاظ بها أكثر مما هو ضروري.
- تمت معالجتها وفقًا لحقوق صاحب البيانات.
- مؤمنة.
- ينقل للآخرين مع الحماية الكافية.

يجب على الموظفين التأكد من التالي:

- الحرص في جميع الأوقات على ضمان حفظ البيانات الشخصية بشكل آمن، وتقليل أخطار فقدانها أو إساءة استخدامها.
- استخدام البيانات الشخصية فقط على أجهزة حاسوب آمنة ومحمية بكلمة مرور وأجهزة أخرى، مع التأكد من تسجيل خروجهم بشكل صحيح في نهاية أي جلسة يستخدمون فيها البيانات الشخصية.
- نقل البيانات باستخدام التشفير وتأمين الأجهزة المحمية بكلمة مرور.
- عند تخزين البيانات الشخصية على أي نظام حاسوب محمول أو محرك أقراص **USB** أو أي وسائط أخرى قابلة للإزالة:

➢ يجب أن تكون البيانات مشفرة ومحمية بكلمة مرور.
➢ يجب أن يكون الجهاز محميًا بكلمة مرور (لا يمكن حماية العديد من بطاقات / بطاقات الذاكرة والأجهزة المحمولة الأخرى بكلمة مرور).
➢ يجب أن يقدم الجهاز برامج معتمدة لفحص الفيروسات والبرامج الضارة.
➢ يجب حذف البيانات بشكل آمن من الجهاز، بما يتماشى مع سياسة المدرسة (أدناه) بمجرد نقلها أو اكتمال استخدامها.

1.2 الأمان - استخدام الصور الرقمية (بما في ذلك مقاطع الفيديو)

أدى تطوير تقنيات التصوير الرقمي إلى تحقيق فوائد كبيرة للتعلم، مما أتاح للموظفين والطلبة الاستخدام الفوري للصور / اللقطات التي قاموا بتسجيلها بأنفسهم أو تنزيلها من الإنترنت. ومع ذلك، يجب أن يكون الموظفون والطلبة على دراية بالمخاطر المرتبطة بمشاركة الصور ونشر الصور على الإنترنت. قد تظل هذه الصور متاحة على الإنترنت إلى الأبد وقد تسبب ضررًا أو إحراجًا للأفراد على المدى القصير أو الطويل.

- عند استخدام الصور الرقمية، يجب على الموظفين إعلام الطلاب وتثقيفهم حول المخاطر المرتبطة بأخذها واستخدامها، ومشاركتها، ونشرها، وتوزيعها. يجب عليهم التعرف على المخاطر المرتبطة بنشر الصور الخاصة بهم على الإنترنت على سبيل المثال. على مواقع التواصل الاجتماعي.
- يُسمح للموظفين بالتقاط صور رقمية / فيديو لدعم الأهداف التعليمية، ولكن يجب عليهم اتباع سياسات المدرسة المتعلقة بمشاركة وتوزيع ونشر تلك الصور. يجب التقاط هذه الصور فقط على المعدات المدرسية؛ لا ينبغي استخدام المعدات الشخصية للموظفين لهذه الأغراض.
- يجب توخي الحذر عند التقاط الصور الرقمية / الفيديو من أن الطلاب يرتدون ملابس مناسبة ولا يشاركون في الأنشطة التي قد تؤدي إلى الإساءة إلى سمعة الأفراد أو المدرسة.
- يجب على الطلاب عدم التقاط صور للآخرين، أو استخدامها، أو مشاركتها، أو نشرها، أو توزيعها دون إذن منهم.
- سيتم اختيار الصور الفوتوغرافية المنشورة على الموقع الإلكتروني أو في أي مكان آخر يتضمن الطلاب بعناية وستتوافق مع إرشادات الممارسات الجيدة بشأن استخدام مثل هذه الصور.
- لن يتم استخدام الأسماء الكاملة للطلاب في أي مكان على الموقع الالكتروني أو مدونة، لا سيما فيما يتعلق بالصور.
- سيتم الحصول على إذن كتابي من أولياء الأمور أو مقدمي الرعاية قبل نشر صور الطلاب على الموقع الالكتروني للمدرسة.
- لا يمكن نشر عمل الطالب إلا بإذن من الطالب وأولياء الأمور أو مقدمي الرعاية.

1.3 الخصوصية الشخصية

يتحمل الموظفون والطلاب مسؤولية ضمان حماية معلوماتهم الشخصية عبر الإنترنت لمنع الآخرين من استخدام هذه المعلومات للوصول إلى التفاصيل الخاصة بك أو انتحال شخصيتك. يجب أن تتضمن تدابير حماية خصوصيتك ما يلي:

- توقف وفكر قبل مشاركة أي معلومات شخصية أو مالية - عنك أو عن أصدقائك أو عائلتك. لا تفصح عن معلومات الهوية (رخصة القيادة، تاريخ الميلاد، العنوان) عبر البريد الإلكتروني أو عبر الإنترنت ما لم تكن قد بدأت الاتصال وتعرف الشخص الآخر المعني.
- إذا كنت تستخدم مواقع الشبكات الاجتماعية، فاضبط إعدادات الخصوصية لديك للتحكم في كمية ونوع المعلومات التي تريد مشاركتها، حتى يتمكن الأشخاص الذين لا تعرفهم جيدًا من رؤية أجزاء معينة فقط من ملفك الشخصي.
- لا تعطي عنوان بريدك الإلكتروني دون الحاجة إلى ذلك. فكر في سبب تقديمك له، وما هي الفائدة بالنسبة لك وما إذا كان ذلك سيعني أنه تم إرسال رسائل بريد إلكتروني لا تريدها.
- قبل إعطاء عنوان بريدك الإلكتروني عبر الإنترنت، اقرأ سياسة الخصوصية الخاصة بالموقع. يجب أن يخبرك هذا كيف سيستخدمون عنوان البريد الإلكتروني الذي قدمته.
- إذا كنت تستخدم عنوان بريدك الإلكتروني غالبًا عبر الإنترنت، فقد ترغب في الحصول على حساب بريد إلكتروني ثانوي. استخدم بريدك الإلكتروني الأساسي مع الأصدقاء والشركات التي تعرفها وتثق بها.
- قم بتعيين كلمات مرور قوية، خاصةً للحسابات المهمة عبر الإنترنت وقم بتغييرها بانتظام، وفكر في عمل إدخال مذكرات لتذكير نفسك.

2. إساءة استخدام الكمبيوتر:

2.1 أعضاء هيئة التدريس والدعم

- يتحملون مسؤولية ضمان أن لديهم وعيًا محدثًا بمسائل السلامة الإلكترونية وسياسة وممارسات السلامة الإلكترونية الحالية في المدرسة.
- يقومون بالإبلاغ عن أي سوء استخدام أو مشكلة مشتبه بها لرئيس تكنولوجيا المعلومات والاتصالات أو رئيس السنة للتحقيق / اتخاذ إجراء / معاقبة.
- يجب أن تكون الاتصالات الرقمية مع الطلبة عبر البريد الإلكتروني **/ ClassDojo /** بيئة التعلم الافتراضية **/ (VLE)** الصوت على مستوى احترافي ويتم إجراؤها فقط باستخدام أنظمة المدرسة الرسمية. لا يُسمح للمعلمين بالدخول في رسائل نصية أو أي مجموعات مثل **WhatsApp** مع الطلاب أو أولياء الأمور.
- يتم تضمين قضايا السلامة الإلكترونية في جميع جوانب المناهج والأنشطة المدرسية الأخرى.
- يفهم الطلاب ويتبعون السلامة الإلكترونية للمدرسة وسياسة الاستخدام المقبول.
- يتمتع الطلاب بفهم جيد لمهارات البحث والحاجة إلى تجنب الانتحال ودعم لوائح حقوق النشر.
- يراقبون نشاط تكنولوجيا المعلومات والاتصالات في الدروس والأنشطة المدرسية اللامنهجية والموسعة.

- يجب أن يكونوا على دراية بقضايا السلامة الإلكترونية المتعلقة باستخدام الهواتف المحمولة والكاميرات والأجهزة المحمولة باليد وأنهم يراقبون استخدامها وينفذون سياسات المدرسة الحالية فيما يتعلق بهذه الأجهزة.
- في الدروس التي يكون فيها استخدام الإنترنت مخططًا مسبقًا، يجب توجيه الطلاب إلى المواقع التي تم التحقق منها على أنها مناسبة لاستخدامها وأن العمليات موجودة للتعامل مع أي مادة غير مناسبة توجد في عمليات البحث على الإنترنت.

2.2 الطلبة

- يتحملون مسؤولية استخدام أنظمة تكنولوجيا المعلومات والاتصالات في المدرسة وفقًا لسياسة الاستخدام المقبول للطالب، والتي يُتوقع منهم التوقيع عليها (بواسطة ولي الأمر / الوصي) قبل منحهم حق الوصول إلى أنظمة المدرسة.
- لديك فهم جيد لمهارات البحث والحاجة إلى تجنب الانتحال ودعم لوائح حقوق النشر.
- تحتاج إلى فهم أهمية الإبلاغ عن إساءة الاستخدام أو سوء الاستخدام أو الوصول إلى مواد غير مناسبة ومعرفة كيفية القيام بذلك.
- من المتوقع معرفة وفهم سياسات المدرسة بشأن استخدام الهواتف المحمولة والكاميرات الرقمية والأجهزة المحمولة. يجب عليهم أيضًا معرفة وفهم سياسات المدرسة بشأن التقاط / استخدام الصور والتسلط عبر الإنترنت. (التنمر الإلكتروني هو استخدام الاتصالات الإلكترونية للتنمر على شخص ما، عادةً عن طريق إرسال رسائل ذات طبيعة تخويف أو تهديد).
- يجب فهم أهمية تبني ممارسات السلامة الإلكترونية الجيدة عند استخدام التقنيات الرقمية خارج المدرسة وإدراك أن سياسة السلامة الإلكترونية للمدرسة تغطي أفعالهم خارج المدرسة، إذا كانت مرتبطة ببعضهم في المدرسة.
- يجب الامتناع عن أي نشاط عبر الإنترنت خارج ساعات الدوام المدرسي، مما قد يكون له تأثير سلبي داخل البيئة المدرسية.

2.3 أولياء الأمور / مقدمو الرعاية / الأوصياء

يلعب أولياء الأمور دورًا مهمًا في ضمان فهم أطفالهم للحاجة إلى استخدام الإنترنت / الأجهزة المحمولة بطريقة مناسبة. تظهر الأبحاث أن العديد من الآباء ومقدمي الرعاية لا يفهمون تمامًا القضايا وأنهم أقل خبرة في استخدام تكنولوجيا المعلومات والاتصالات من أطفالهم. لذلك، ستنتهز المدرسة كل فرصة لمساعدة أولياء الأمور على فهم هذه القضايا من خلال اجتماعات أولياء الأمور، والنشرات الإخبارية ، والرسائل ، وموقع الويب **VLE /** ومعلومات حول حملات / أدبيات السلامة الإلكترونية الوطنية / المحلية. سيكون الآباء ومقدمو الرعاية مسؤولين عن:

- الموافقة (بالتوقيع) على سياسة الاستخدام المقبول للطالب.
- الوصول إلى موقع المدرسة **/ VLE /** سجلات الطلاب عبر الإنترنت وفقًا لسياسة الاستخدام المقبول الخاصة بالمدرسة ذات الصلة.

2.4 التقنية - البنية التحتية / المعدات والمراقبة

تعد المدرسة مسؤولة عن ضمان أن البنية التحتية / شبكة المدرسة آمنة ومأمونة بقدر الإمكان بشكل معقول وأن السياسات والإجراءات المعتمدة في هذه السياسة يتم تنفيذها. ستحتاج أيضًا إلى التأكد من أن الأشخاص المعنيين المذكورين في الأقسام المذكورة أعلاه سيكونون فعالين في تنفيذ مسؤوليات السلامة الإلكترونية الخاصة بهم:

- تتم إدارة أنظمة تكنولوجيا المعلومات والاتصالات بالمدرسة بطرق تضمن استيفاء المدرسة للمتطلبات الفنية للسلامة الإلكترونية الموضحة في سياسة الاستخدام المقبول.
- تكون هناك مراجعات ومراجعات منتظمة لسلامة وأمن أنظمة تكنولوجيا المعلومات والاتصالات في المدارس.
- يجب وضع الخوادم والأنظمة اللاسلكية والكابلات في مكان آمن مع تقييد الوصول المادي.
- يكون لجميع المستخدمين حقوق وصول محددة بوضوح إلى أنظمة تكنولوجيا المعلومات والاتصالات في المدارس. سيتم تسجيل تفاصيل حقوق الوصول المتاحة لمجموعات المستخدمين بواسطة مدير الشبكة (أو أي شخص آخر) وسيراجعها مدير الشبكة، سنويًا على الأقل.
- يتم تزويد جميع المستخدمين باسم مستخدم وكلمة مرور بواسطة مدير الشبكة الذي سيحتفظ بسجل محدث للمستخدمين وأسماء المستخدمين الخاصة بهم. سيُطلب من المستخدمين تغيير كلمة المرور الخاصة بهم بانتظام.

- يكون المستخدمون مسؤولين عن أمان اسم المستخدم وكلمة المرور الخاصة بهم. يجب ألا يسمحوا للمستخدمين الآخرين بالوصول إلى الأنظمة باستخدام تفاصيل تسجيل الدخول الخاصة بهم ويجب عليهم الإبلاغ فورًا عن أي شك أو دليل على حدوث خرق للأمن.
- تحافظ المدرسة على خدمة التصفية المُدارة وتدعمها. قدمت المدرسة ترشيحًا محسنًا على مستوى المستخدم.
- في حالة احتياج مدير الشبكة (أو أي شخص آخر) إلى إيقاف تشغيل التصفية لأي سبب، أو لأي مستخدم، يجب تسجيل ذلك وتنفيذه من خلال عملية يتفق عليها مدير المدرسة المعني (أو غيره من المرشحين) قيادي بارز.(
- ينظر مدير الشبكة والمدير في الطلبات الواردة من الموظفين بشأن المواقع المراد إزالتها من القائمة التي تمت تصفيتها. إذا تمت الموافقة على الطلب، فسيتم تسجيل هذا الإجراء ومراجعة سجلات هذه الإجراءات بانتظام.
- يقوم الطاقم الفني لتكنولوجيا المعلومات والاتصالات في المدرسة بمراقبة وتسجيل نشاط المستخدمين على أنظمة تكنولوجيا المعلومات والاتصالات بالمدرسة بشكل منتظم ويتم إعلام المستخدمين بذلك في سياسة الاستخدام المقبول.
- يوجد نظام مناسب (سيتم وصفه) للمستخدمين للإبلاغ عن أي حادث أمان إلكتروني فعلي / محتمل إلى مدير الشبكة (أو أي شخص آخر ذي صلة).
- يتم اتخاذ تدابير أمنية مناسبة لحماية الخوادم وجدران الحماية وأجهزة التوجيه والأنظمة اللاسلكية ومحطات العمل والأجهزة المحمولة باليد وما إلى ذلك من المحاولات العرضية أو الخبيثة التي قد تهدد أمن أنظمة المدرسة وبياناتها.
- تتم حماية البنية التحتية للمدرسة ومحطات العمل الفردية بواسطة برنامج فيروسات محدث.
- لا يمكن إرسال البيانات الشخصية عبر الإنترنت أو إزالتها من موقع المدرسة ما لم يتم تشفيرها بأمان أو تأمينها بطريقة أخرى.

3. آداب التواصل الاجتماعي

يجب اتباع آداب الشبكات الاجتماعية عند الاتصال والتفاعل على الإنترنت. يجب اتباع قواعد آداب السلوك التالية:

- لا تستخدم مطلقًا لغة تهديد، أو تشهير، أو بذيئة، أو بذيئة عند التواصل عبر الإنترنت.
- لا ترد على الرسائل الوقحة أو التهديدية سواء في الدردشة، أو المنتديات، أو التعليقات، أو لوحات الرسائل.
- غادر دائمًا إذا كانت المحادثة تجعلك غير مرتاح.
- لا تنخرط في "ملتهب" - أي معركة عدوانية عبر الإنترنت أو إهانات بين شخصين أو أكثر.
- لا ترسل رسائل بريد إلكتروني بأحرف كبيرة - فهذا يعتبر صراخًا. • يجب ألا تقول أشياء بذيئة أو غير صحيحة عن الآخرين خاصة في المنتديات العامة أو مجموعات الأخبار أو الدردشة. تظل هذه في العديد من الأرشيفات وقد يتم اتهامك بالتشهير أو التشهير أو القذف.
- لا تقم أبدًا بإعادة توجيه رسائل البريد الإلكتروني الشخصية المرسلة إليك إلى الآخرين دون التحقق من المرسل الأصلي أولاً.
- وبالمثل، عند إعادة توجيه بريد إلكتروني للآخرين، احترم خصوصية مجموعة الأصدقاء أو العائلة. لا تقم ببث جميع عناوين بريدهم الإلكتروني بشكل عام، استخدم الأمر النسخ السري **(BCC)** للحفاظ على خصوصيتها.

4. الإبلاغ عن السلوك المعادي للمجتمع / السلوك غير القانوني عبر الإنترنت

4.1 السلوك غير القانوني

من المأمول أن يكون جميع أعضاء المجتمع المدرسي مستخدمين مسؤولين لتكنولوجيا المعلومات والاتصالات، والذين يفهمون ويتبعون هذه السياسة. ومع ذلك، قد تكون هناك أوقات يمكن أن تحدث فيها انتهاكات للسياسة، من خلال الإهمال أو غير المسؤول، أو في حالات نادرة جدًا، من خلال سوء الاستخدام المتعمد. المدرجة أدناه هي الردود التي سيتم إجراؤها على أي حوادث إساءة استخدام ظاهرة أو فعلية:

إذا بدا أن أي إساءة استخدام ظاهرة أو فعلية تنطوي على نشاط غير قانوني، أي:

- صور الاعتداء الجنسي على الأطفال.
- المواد الخاصة بالبالغين والتي من المحتمل أن تنتهك قانون المنشورات الفاحشة.
- مادة عنصرية جنائية.
- سلوك أو نشاط أو مواد إجرامية أخرى.

يجب عليك أن:

- إذا كان لديك دليل فعلي، افصل الحاسوب (إن أمكن) من التيار الكهربائي على الفور، ولكن لا تحذف أي دليل.
- إذا كنت واثقًا من عدم مشاركة مدير الشبكة، فتحدث إليه على الفور. وإلا فلا تشركهم وتحدث إلى رئيس الابتدائية أو الثانوية.
- قد تحتاج السلطات المحلية للمشاركة في قرار المدير الأكاديمي.

4.2 السلوك القانوني المعادي للمجتمع

من المرجح أن المدرسة سوف تحتاج إلى التعامل مع الحوادث التي تنطوي على سوء استخدام غير لائق وليس غير قانوني. من المهم أن يتم التعامل مع أي حوادث في أسرع وقت ممكن بطريقة متناسبة، وأن يدرك أعضاء المجتمع المدرسي أنه تم التعامل مع الحوادث. من المقرر أن يتم التعامل مع حوادث سوء الاستخدام من خلال السلوك العادي / الإجراءات التأديبية.

تتعامل المدرسة مع مثل هذه الحوادث ضمن هذه السياسة والسلوك المرتبط بها وسياسات مكافحة التنمر، وستقوم، عند معرفة ذلك، بإبلاغ أولياء الأمور / مقدمي الرعاية بحوادث السلوك غير الملائم للسلامة الإلكترونية التي تحدث داخل المدرسة أو خارجها. سيتم التعامل مع سلوك السلامة الإلكترونية غير المناسب فيما يتعلق بموظفي مدرسة قطر العالمية على أساس كل حالة على حدة.

أثناء التواجد في الموقع، قد يتلقى الطلاب شكلاً من أشكال الإجراءات التأديبية و / أو خطاب تحذير (المستوى 4 من العقوبة) لأي من الأمثلة التالية:

- الوصول غير المصرح به إلى / فقدان / مشاركة المعلومات الشخصية.
- الإدخال المتعمد لفيروس إلى شبكة المدرسة.
- استخدام البيانات الشخصية للطلاب الآخرين.
- تحميل مواد غير لائقة (ألعاب، صور، لغة بذيئة، إلخ) على الشبكة.
- التنمر الإلكتروني.
- الاستخدام غير المناسب للأجهزة الرقمية الشخصية مثل الهواتف المحمولة والأجهزة اللوحية.
- الغش وحقوق المؤلف والانتحال.
- الوصول إلى المحتوى المحظور أو غير الملائم على الإنترنت.
- الوصول إلى صور أو محتوى آخر غير قانوني أو ضار أو غير مناسب.
- مشاركة / توزيع الصور الشخصية دون موافقة أو علم الفرد.
- التنزيل غير القانوني للموسيقى أو ملفات الفيديو.
- استخدام البرامج غير المرخصة / غير الرسمية داخل المدرسة.
- التواصل المجهول غير الملائم مع الأقران.
- نشاط عبر الإنترنت خارج المدرسة قد يكون له تداعيات سلبية داخل المدرسة.

التقييم

نحن نعيش في عالم رقمي حيث التغيير سريع - لدرجة أنه يصعب أحيانًا مواكبة التقنيات الناشئة. مع أخذ ذلك في الاعتبار، يجب مراجعة وتحديث قوانيننا وعقوباتنا باستمرار.

قد تكون هناك، حتمًا، أوقات تتضمن فيها السياسات "مناطق رمادية" معينة أو لا تعالج تغييرات معينة فورية أو قصيرة المدى على طريقة استخدام التقنيات الجديدة. مع أخذ ذلك في الاعتبار، نتحمل جميعًا مسؤولية التعامل مع هذه الموارد بموقف ناضج ومسؤول؛ لمراقبة الطلاب حتى يكونوا آمنين للاستمتاع واكتساب الخبرات الإيجابية من أنشطتهم عبر الإنترنت؛ وأن نتصرف بطريقة تمثل هذه المعايير في جميع الأوقات.

ستتم مراجعة سياسة السلامة الإلكترونية سنويًا، أو بشكل أكثر انتظامًا في ضوء أي تطورات جديدة مهمة في استخدام التقنيات أو التهديدات الجديدة للسلامة الإلكترونية أو الحوادث التي حدثت. تم تقديم تاريخ المراجعة المتوقع التالي في بداية السياسة.