ليـــوا للتعليم
Liwa Education

E-Safety Policy

سياسة السلامة الالكترونية

السياسة

النظرة العامة

من واجب المدرسة ضمان حماية الأطفال والشباب من الأذى المحتمل داخل المدرسة وخارجها. تنطبق سياسة السلامة الإلكترونية على جميع أعضاء المجتمع المدرسي ويجب أن يلتزم بها الجميع (بما في ذلك الموظفين والطلاب / التلاميذ والمتطوعين والآباء / مقدمي الرعاية والزائرين ومستخدمي المجتمع) الذين يمكنهم الوصول إلى المدرسة ومستخدميها. أنظمة تكنولوجيا المعلومات والاتصالات ، داخل وخارج المدرسة. في حالة وجود حادثة تنمر عبر الإنترنت ، أو غيرها من حوادث السلامة الإلكترونية التي تغطيها هذه السياسة ، والتي قد تحدث خارج المدرسة ، ولكنها مرتبطة بعضوية المدرسة ، ستفرض المدرسة عقوبات تأديبية على السلوك غير اللائق حيث يكون ذلك معقولًا على النحو المنصوص عليه في سياسة السلوك بالمدرسة.

ستتعامل المدرسة مع مثل هذه الحوادث ضمن هذه السياسة والسلوكيات المرتبطة بها ، وستقوم ، حيثما كان معروفًا ، بإبلاغ أولياء الأمور / مقدمي الرعاية بحوادث السلوك غير الملائم للسلامة الإلكترونية التي تحدث خارج المدرسة.

أهداف

- للتأكيد على الحاجة إلى تثقيف الموظفين والأطفال والشباب حول إيجابيات وسلبيات استخدام التقنيات الجديدة داخل المدرسة وخارجها.
- توفير ضمانات واتفاق الاستخدام المقبول لإرشاد جميع المستخدمين ، سواء كانوا موظفين أو طلابًا ، في تجاربهم عبر الإنترنت.
- التأكد من أن البالغين على دراية بإجراءات إساءة استخدام أي تقنيات داخل المدرسة وخارجها.
- لتطوير روابط مع أولياء الأمور / مقدمي الرعاية والمجتمع الأوسع لضمان مساهمتهم في السياسات والإجراءات مع استمرار الوعي بالفوائد والقضايا المحتملة المتعلقة بالتقنيات.

تعريفات

يستخدم مصطلح "السلامة الإلكترونية" ليشمل الاستخدام الآمن لجميع التقنيات من أجل حماية الأطفال والشباب والبالغين من المخاطر المحتملة والمعروفة.

الأدوار والإجراءات المعينة

الحكام والمديرين

تقع على عاتق المديرين مسؤولية ضمان فهم الحكام لمسؤولياتهم والحصول على نظرة عامة على السلامة الإلكترونية كجزء من الاختصاص الأوسع للحماية عبر المدرسة مع مزيد من المسؤوليات على النحو التالي:

- عيّن المدير مسؤولاً عن السلامة الإلكترونية لتنفيذ السياسات والإجراءات المتفق عليها وتدريب الموظفين ومتطلبات المناهج وتحمل المسؤولية لضمان معالجة السلامة الإلكترونية من أجل إنشاء بيئة تعليمية آمنة لتكنولوجيا المعلومات والاتصالات. جميع الموظفين والطلاب على دراية بالشخص الذي تم تعيينه لهذا الدور داخل المدرسة.
- يوجد إخلاء مسؤولية قياسي في جميع رسائل البريد الإلكتروني ينص على أن الآراء المعبر عنها ليست بالضرورة آراء المدرسة أو المنظمة.
- يجب توفير الموارد لموظف السلامة الإلكترونية ليتم تدريبه بمعلومات محدثة حتى يتمكنوا من تحديث السياسات ، عند الاقتضاء.
- يتحمل جميع الموظفين مسؤولية تعزيز السلامة الإلكترونية عبر المناهج الدراسية

مسؤول السلامة الإلكترونية

دور مسؤول السلامة الإلكترونية المعين هو:

- ❑ تعزيز أهمية السلامة الإلكترونية داخل المدرسة كجزء من واجبها في الرعاية لضمان سلامة تلاميذها وموظفيها.
- ❑ إنشاء والحفاظ على بيئة تعليمية آمنة لتكنولوجيا المعلومات والاتصالات داخل المدرسة.
- ❑ تأكد من مراجعة اتفاقيات الاستخدام المقبول سنويًا ، بمعلومات محدثة ، وأن التدريب متاح للموظفين لتعليم السلامة الإلكترونية وللآباء ليشعروا بأنهم على علم ومعرفة إلى أين يذهبون للحصول على المشورة.
- ❑ اعمل جنبًا إلى جنب مع مدير الشبكة لضمان ضبط التصفية على المستوى الصحيح للموظفين والأطفال والشباب.
- ❑ تجهيز (أي تدريب) الأطفال ليظلوا آمنين عبر الإنترنت ، سواء في المدرسة أو خارج المدرسة.
- ❑ تأكد من أن جميع البالغين على دراية بمستويات التصفية ولماذا هم هناك لحماية الأطفال والشباب.
- ❑ الاتصال بـ Cyber Safety PLC لمناقشة وتخفيف اتجاهات السلامة الإلكترونية أو التهديدات المحددة داخل المدرسة بحيث تكون السياسات والإجراءات محدثة لمراعاة أي مشكلات وتقنيات ناشئة.
- ❑ قم بتحديث الموظفين حول التقنيات الجديدة والناشئة بحيث يمكن تدريس معلومات السلامة الإلكترونية الصحيحة أو الالتزام بها.
- ❑ الإشراف على المراقبة الشفافة للإنترنت والتقنيات عبر الإنترنت. يوفر نظام جدار حماية الإنترنت بالمدرسة أيضًا مستوى عالٍ من المراقبة الشفافة كجزء من وظائفه.

- ❑ قم بتحليل سجلات حوادث السلامة الإلكترونية بانتظام للمساعدة في إبلاغ التطوير والحماية في المستقبل ، حيث يمكن تحديد المخاطر.
- ❑ العمل جنبًا إلى جنب مع مدير الشبكة لضمان وجود برامج مكافحة فيروسات وبرامج مكافحة التجسس المناسبة

- ❑ والحديثة على الشبكة ، وأجهزة الكمبيوتر الشخصية المستقلة وأجهزة الكمبيوتر المحمولة الخاصة بالمدرس / الأطفال ، وأن تتم مراجعة هذا وتحديثه على أساس منتظم .
- ❑ تأكد من تقليل رسائل البريد الإلكتروني غير المرغوب فيها إلى أحد الموظفين من مصادر أخرى.
- ❑ تقديم المشورة بشأن مراجعة منهج السلامة الإلكترونية للتأكد من أنه محدث لمراعاة أي قضايا وتقنيات ناشئة.
- ❑ تقديم تقارير منتظمة إلى فريق القيادة العليا.

مسؤول السلامة الإلكترونية - الوصف الوظيفي

- ❑ تطوير ثقافة السلامة الإلكترونية تحت إشراف فريق الإدارة والعمل كنقطة اتصال محددة في جميع قضايا السلامة الإلكترونية.
- ❑ التأكد من أن كل شخص بما في ذلك الأطفال والشباب يعرفون ماذا يفعلون إذا كانوا قلقين بشأن مشكلة تتعلق بالسلامة الإلكترونية.
- ❑ التأكد من أن السلامة الإلكترونية مضمنة في التطوير المهني المستمر (CPD) للموظفين وتنسيق التدريب حسب الاقتضاء.
- ❑ ضمان أن يتم تضمين السلامة الإلكترونية في جميع المناهج الدراسية وفي جميع الأنشطة المعنية حسب الاقتضاء.
- ❑ ضمان تعزيز السلامة الإلكترونية الآباء ومقدمي الرعاية والمستخدمين الآخرين لتكنولوجيا المعلومات والاتصالات داخل مجتمع ليوا.
- ❑ ضمان توفير الموارد الكافية لجميع الطلاب لدعمهم في فهمهم لجميع القضايا المتعلقة بالسلامة الإلكترونية.
- ❑ الاحتفاظ بسجل حوادث السلامة الإلكترونية.
- ❑ المراقبة والإبلاغ عن قضايا السلامة الإلكترونية لفريق الإدارة والوكالات الأخرى حسب الاقتضاء.
- ❑ تطوير فهم للإرشادات المحلية والوطنية ذات الصلة.
- ❑ بالتشاور مع SLT ، التنسيق مع السلطات المحلية حسب الاقتضاء.
- ❑ مراجعة وتحديث سياسات وإجراءات السلامة الإلكترونية بشكل دوري وبعد وقوع أي حادث.
- ❑ تأكد من مشاركة نتائج التعلم والتعليقات بشكل مناسب.
- ❑ التأكد من أن البنية التحتية والتكنولوجيا توفر بيئة آمنة ومأمونة للجميع داخل مجتمع ليوا.
- ❑ تأكد من أن المدرسة لديها
  - ❑ جدران الحماية.
  - ❑ برامج مكافحة الفيروسات وبرامج التجسس.
  - ❑ المرشحات.

- ❑ الوعي بأي قضايا تقنية لاسلكية.
- ❑ سياسة واضحة لاستخدام الأجهزة الشخصية.

لجنة التعليم المهني للسلامة الإلكترونية.

تقع على عاتق اللجنة داخل المدرسة مسؤولية:

- ❑ مراجعة جميع السياسات والبروتوكولات المتعلقة بالسلامة الإلكترونية.
- ❑ تأكد من أن جميع المدارس لديها برنامج تدريبي للسلامة الإلكترونية
- ❑ تأكد من قيام المعلمين بتطبيق دروس السلامة الإلكترونية في دروسهم المستمرة.
- ❑ تأكد من أن بيئة المدرسة آمنة ومأمونة وأن بروتوكولات السلامة المناسبة مطبقة.
- ❑ التخطيط لأحداث مجتمعية منتظمة تتعلق بالسلامة الإلكترونية.

مسؤول حماية البيانات

دور مسؤول السلامة الإلكترونية المعين هو:

- ❑ توفير التدريب على متطلبات الامتثال
- ❑ توفير التدريب للموظفين المشاركين في معالجة البيانات
- ❑ إجراء عمليات تدقيق لضمان الامتثال ومعالجة المشكلات المحتملة بشكل استباقي
- ❑ العمل كنقطة اتصال بين المدرسة والسلطات التنظيمية.
- ❑ مراقبة الأداء وتقديم المشورة بشأن تأثير جهود حماية البيانات
- ❑ الاحتفاظ بسجلات شاملة لجميع أنشطة معالجة البيانات التي تجريها المدرسة ، بما في ذلك أغراض جميع أنشطة المعالجة ، والتي يجب أن تكون متاحة للجمهور عند الطلب
- ❑ التواصل مع موضوعات البيانات لإبلاغهم بكيفية استخدام بياناتهم ، وحقهم في محو بياناتهم الشخصية ، وما هي الإجراءات التي اتخذتها الشركة لحماية معلوماتهم الشخصية.
- ❑ حماية البيانات: الوصف الوظيفي
- ❑ فهم قانون حماية البيانات (المحتويات والتفسير) وكيف يتم تطبيقه ومواءمته مع سياسة حماية البيانات بالمدرسة.
- ❑ تفسير المتطلبات التنظيمية وتقديم المشورة حول كيفية تطبيق ذلك داخل المدرسة.
- ❑ الاتصال مع النظراء الخارجيين (المنظمين) وكذلك أصحاب المصلحة الداخليين لدعم تنفيذ سياسة حماية بيانات المدرسة بما يتوافق مع قانون دولة الإمارات العربية المتحدة.
- ❑ توفير تدريب موظفي التوعية بشأن حماية البيانات لجميع أصحاب المصلحة.
- ❑ مسؤول مراقبة بيانات السلامة الإلكترونية

- ❑ دور مسؤول السلامة الإلكترونية المعين هو:
- ❑ إنشاء وتنسيق نظام مراقبة السلامة الإلكترونية بما في ذلك جمع البيانات وتحليلها ومراجعتها.
- ❑ تحديد مؤشرات انتهاك السلامة الإلكترونية المناسبة ، وكيفية مراقبتها ومراجعتها.
- ❑ العمل عن كثب مع الفرق ذات الصلة (مسؤول الشبكة ومنسق التعلم الإلكتروني وفريق إدارة الأجهزة) لإعداد طرق وأدوات محددة لجمع البيانات

- ❑ تنسيق أنشطة المراقبة والمدخلات المطلوبة من أعضاء الفريق الآخرين.
- ❑ توقع وتخطيط ودعم متطلبات إعداد التقارير.
- ❑ ضمان مشاركة المعلومات التي تم جمعها من خلال أنشطة المراقبة بسرعة وفيتنسيق مناسب مع مسؤول السلامة الإلكترونية بحيث يمكن معالجة أي مشاكل تنشأ.

الموظفين والكبار

تقع على عاتق جميع البالغين داخل المدرسة مسؤولية:

- تأكد من أن مستويات التصفية مناسبة للتلاميذ وأنها مضبوطة على المستوى الصحيح وقم بإبلاغ مسؤول السلامة الإلكترونية بأي مخاوف.
- تنبيه مسؤول السلامة الإلكترونية إلى أي مشاكل ومخاطر جديدة أو ناشئة قد تحتاج إلى إدراجها في السياسات والإجراءات.
- تأكد من أن جميع الطلاب محميون ومدعومون في استخدامهم للتقنيات حتى يعرفوا كيفية استخدامها بطريقة آمنة ومسؤولة. يجب أن يعرف جميع التلاميذ ما يجب عليهم فعله في حالة وقوع حادث.
- كن على اطلاع دائم بمعرفة السلامة الإلكترونية المناسبة للفئة العمرية وتعزيزها من خلال المناهج الدراسية.
- قم بالإبلاغ عن الوصول غير المقصود إلى المواد غير الملائمة إلى مسؤول السلامة الإلكترونية من أجل إضافة المواقع غير الملائمة إلى القائمة المقيدة.
- استخدم برنامج مكافحة الفيروسات وتحقق من وجود فيروسات على الكمبيوتر المحمول الخاص بالعمل أو شريحة الذاكرة أو قرص مضغوط عند نقل المعلومات من الإنترنت بشكل منتظم ، خاصةً عندما لا تكون متصلاً بإعداد المدرسة / التعليم أو شبكة مؤسسة أخرى.
- تأكد من تخزين جميع المعلومات الحساسة فقط على شبكة المدرسة ولا يمكن الوصول إليها إلا من قبل المستخدمين المصادق عليهم داخل نطاق المدرسة كما هو مذكور في سياسة حماية البيانات. (يجب عدم حفظ أي بيانات حساسة على محركات الأقراص المحلية أو أجهزة التخزين الشخصية.)
- قم بالإبلاغ عن حوادث "التنمر" الموجهة شخصيًا أو أي سلوك غير لائق آخر عبر الإنترنت أو تقنيات أخرى إلى مسؤول السلامة الإلكترونية.
- اعلم أنه من خلال تقديم نموذج سياسة المدرسة عبر الإنترنت ، فإنك توافق على الالتزام بشروط السياسة.
- كن 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 ، حيث يكون استخدام الإنترنت مخططًا مسبقًا ، يجب توجيه الطلاب / التلاميذ 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.

.

التلاميذ

تقع على عاتق جميع التلاميذ داخل المدرسة مسؤولية:

- كن مستخدمين مسؤولين لأنظمة تكنولوجيا المعلومات والاتصالات بالمدرسة وفقًا لسياسة الاستخدام المقبول للمدرسة.
- لفهم أهمية الإبلاغ عن إساءة الاستخدام أو إساءة الاستخدام أو الوصول إلى مواد غير ملائمة ومعرفة كيفية القيام بذلك.
- لفهم سياسات المدرسة بشأن استخدام الهواتف المحمولة والكاميرات الرقمية والأجهزة المحمولة باليد. (سياسات التقاط / استخدام الصور والتسلط عبر الإنترنت.
- اعتماد ممارسة جيدة للسلامة الإلكترونية عند استخدام التقنيات الرقمية خارج المدرسة وإدراك أن سياسة السلامة الإلكترونية بالمدرسة تغطي أفعالهم خارج المدرسة ، إذا كانت مرتبطة بعضويتهم في المدرسة.
- لديك فهم جيد لمهارات البحث والحاجة إلى تجنب الانتحال ودعم لوائح حقوق النشر.

الضيوف / الزوار

- ❑ تقع على عاتق جميع الضيوف داخل المدرسة مسؤولية:
- ❑ افهم أنه لا يتم منح الضيوف إمكانية الوصول إلى أنظمة المدرسة باستثناء شبكة WiFi.
- ❑ استخدم أنظمة المدرسة وأجهزتها ، بما في ذلك شبكتها اللاسلكية ، بطريقة مسؤولة ، للتأكد من عدم وجود خطر على سلامة الطلاب أو على سلامة وأمن الأنظمة والأجهزة والمستخدمين الآخرين.
- ❑ قم بالإبلاغ عن الوصول غير المقصود إلى المواد غير الملائمة إلى مسؤول السلامة الإلكترونية من أجل إضافة المواقع غير الملائمة إلى القائمة المقيدة.

التنفيذ التشغيلي

التعليم - جميع الطلاب

في حين أن الحلول التنظيمية والتقنية مهمة جدًا ، يجب أن يكون استخدامها متوازنًا من خلال تثقيف جميع الطلاب لاتخاذ نهج مسؤول. لذلك ، يعد تعليم الطلاب والقائمين على رعايتهم في مجال السلامة الإلكترونية جزءًا أساسيًا من توفير السلامة الإلكترونية لدينا.

سيتم توفير تعليم السلامة الإلكترونية بالطرق التالية:

- ❑ يتم توفير برنامج السلامة الإلكترونية المخطط كجزء من منهج تكنولوجيا المعلومات والاتصالات ومن خلال PACE (التعليم الشخصي والمجتمعي).
- ❑ تتم إعادة زيارة المنهج بانتظام لتغطية استخدام تكنولوجيا المعلومات والاتصالات والتقنيات الجديدة في المدرسة وخارج المدرسة. يتم تعزيز رسائل السلامة الإلكترونية الرئيسية كجزء من برنامج مخطط للتجمعات والأنشطة التعليمية / الرعوية.
- ❑ يتم تعليم الطلاب في جميع الدروس ليكونوا على دراية نقدية بالمواد / المحتوى الذي يصلون إليه عبر الإنترنت ويتم توجيههم للتحقق من دقة المعلومات.
- ❑ يتم تشجيع الطلاب على اعتماد الاستخدام الآمن والمسؤول لتكنولوجيا المعلومات والاتصالات والإنترنت والأجهزة المحمولة داخل المدرسة وخارجها.
- ❑ يتم تعليم الطلاب التعرف على مصدر المعلومات المستخدمة واحترام حقوق النشر عند استخدام المواد التي يتم الوصول إليها على الإنترنت.
- ❑ تم نشر قواعد استخدام أنظمة تكنولوجيا المعلومات والاتصالات / الإنترنت في جميع الغرف.
- ❑ يُطلب من الموظفين أن يكونوا قدوة جيدة في استخدامهم لتكنولوجيا المعلومات والاتصالات والإنترنت والأجهزة المحمولة.

تعليم وتدريب الموظفين

من الضروري أن يتلقى موظفونا تدريبًا على السلامة الإلكترونية وأن يفهموا مسؤولياتهم ، مثل المبينة في هذه السياسة:

- ❑ يتم توفير تدريب السلامة الإلكترونية للموظفين كجزء من برنامجنا التعريفي في بداية العام الدراسي وعلى مدار العام كما هو مطلوب.
- ❑ يتم تحديث جميع الموظفين بانتظام بتطورات السلامة الإلكترونية ذات الصلة
- ❑ يتم تقديم سياسة السلامة الإلكترونية هذه ومناقشتها من قبل الموظفين في اجتماعات الموظفين / الفريق / أيام INSET.
- ❑ سيقدم موظف السلامة الإلكترونية المشورة / التوجيه / التدريب للأفراد كما هو مطلوب.

التعليم - مجتمع ليوا

- ❑ نحن نقدر المساهمة التي يقدمها المجتمع الأوسع في ضمان سلامة طلابنا ، وعلى هذا النحو سنستمر في دعم مجتمع ليوا الأوسع في جميع الأمور المتعلقة بالسلامة الإلكترونية.
- ❑ سيتم توفير تحديثات منتظمة للآباء بشأن التهديدات الحالية للسلامة الإلكترونية وكيف يمكنهم حماية أنفسهم وعائلاتهم.
- ❑ سيتم توفير تدريب أساسي على السلامة الإلكترونية حول كيفية تأمين الحسابات وضبط / التحقق من إعدادات الخصوصية.
- ❑ تحديثات / تذكيرات منتظمة حول كيفية الإبلاغ عن أي مشاكل / مخاوف تتعلق بالسلامة الإلكترونية في المدرسة.
- ❑ نصائح حول كيفية مراقبة أو إدارة ما يفعله أطفالهم عبر الإنترنت بما في ذلك إدارة وقت الشاشة.

المناهج الدراسية

- ❑ يعد الأمن السيبراني والأخلاقيات مكونًا رئيسيًا لمنهج تكنولوجيا المعلومات والاتصالات لجميع الصفوف (K-12) ، وتضمن الكفاءات الرئيسية التقدم عبر الدرجات وتتوافق مع نتائج الدرجات المتوقعة.
- ❑ السلامة الإلكترونية هي محور التركيز في جميع مجالات المناهج ويجب على الموظفين تعزيز رسائل السلامة الإلكترونية في استخدام التكنولوجيا عبر المناهج الدراسية.
- ❑ في الدروس ، حيث يكون استخدام الإنترنت مخططًا مسبقًا ، من أفضل الممارسات أن يتم توجيه الطلاب إلى المواقع التي تم التحقق منها على أنها مناسبة لاستخدامهم.
- ❑ يتم حظر معظم المواقع افتراضيًا بواسطة تصفية الشبكة ويجب على المدرسين تقديم طلب حتى يتم منح الوصول للطلاب. يتم فحص جميع المواقع قبل منح الإذن.
- ❑ حيث يمكن للطلاب البحث في الإنترنت بحرية ، على سبيل المثال باستخدام محركات البحث ، يجب أن يكون الموظفون يقظين في مراقبة محتوى المواقع التي يزورها الشباب.

- ❑ يجب تعليم الطلاب في جميع الدروس ، ليكونوا على دراية تامة بالمواد / المحتوى الذي يصلون إليه عبر الإنترنت ويتم توجيههم للتحقق من دقة المعلومات
- ❑ يجب تعليم الطلاب التعرف على مصدر المعلومات المستخدمة واحترام حقوق النشر عند استخدام المواد التي يتم الوصول إليها على الإنترنت.

تنفيذ سياسة كلمة المرور

1. كلمات مرور الموظفين والطلاب
2. يتم إصدار كلمة مرور مؤقتة لجميع المستخدمين عندما يتم إنشاء البريد الإلكتروني ومشاركته في البداية.
3. تم إنشاء رسائل البريد الإلكتروني حاليًا لجميع الطلاب في الصفوف 3-12 والموظفين.
4. بمجرد إنشاء الحساب ، يُطلب من المستخدمين على الفور تغيير كلمة المرور الخاصة بهم.
5. يقترح النظام القوة الموصى بها والمعايير المقبولة لكلمة المرور ؛ لا يتم قبول كلمات المرور التي لا تستوفي المعايير.
6. في حالة نسيان كلمة المرور أو الحاجة إلى إعادة تعيين كلمة المرور إذا تم اختراقها ، فسيتم إرسال طلب لإعادة تعيين كلمة المرور من قبل أولياء الأمور إلى المدرسة باستخدام قنوات الاتصال بالمدرسة لطلب إعادة التعيين. ثم تتم مشاركة كلمة المرور الجديدة مع الوالد الذي طلب إعادة التعيين.
7. يمكن للموظفين طلب المعلومات مباشرة من فريق تكنولوجيا المعلومات عن طريق الاتصال بهم على رقم هاتف دعم المدرسة.
8. سيتم تطبيق تحديث كلمة المرور مرتين في العام لجميع الطلاب في الصفوف 3-12 وكل 90 يومًا للموظفين.
9. سيتم تعيين جميع كلمات المرور لطلاب الصف الثاني في الروضة مرة واحدة في العام وسيتم إرسال جميع كلمات المرور إلى أولياء الأمور من قبل مدرس الفصل عبر ClassDojo.
10. لا توجد قاعدة بيانات للموظفين أو كلمات مرور الطلاب متوفرة ، دعم تكنولوجيا المعلومات لديه خيار إعادة التعيين فقط.

وصول الضيف / الزائر

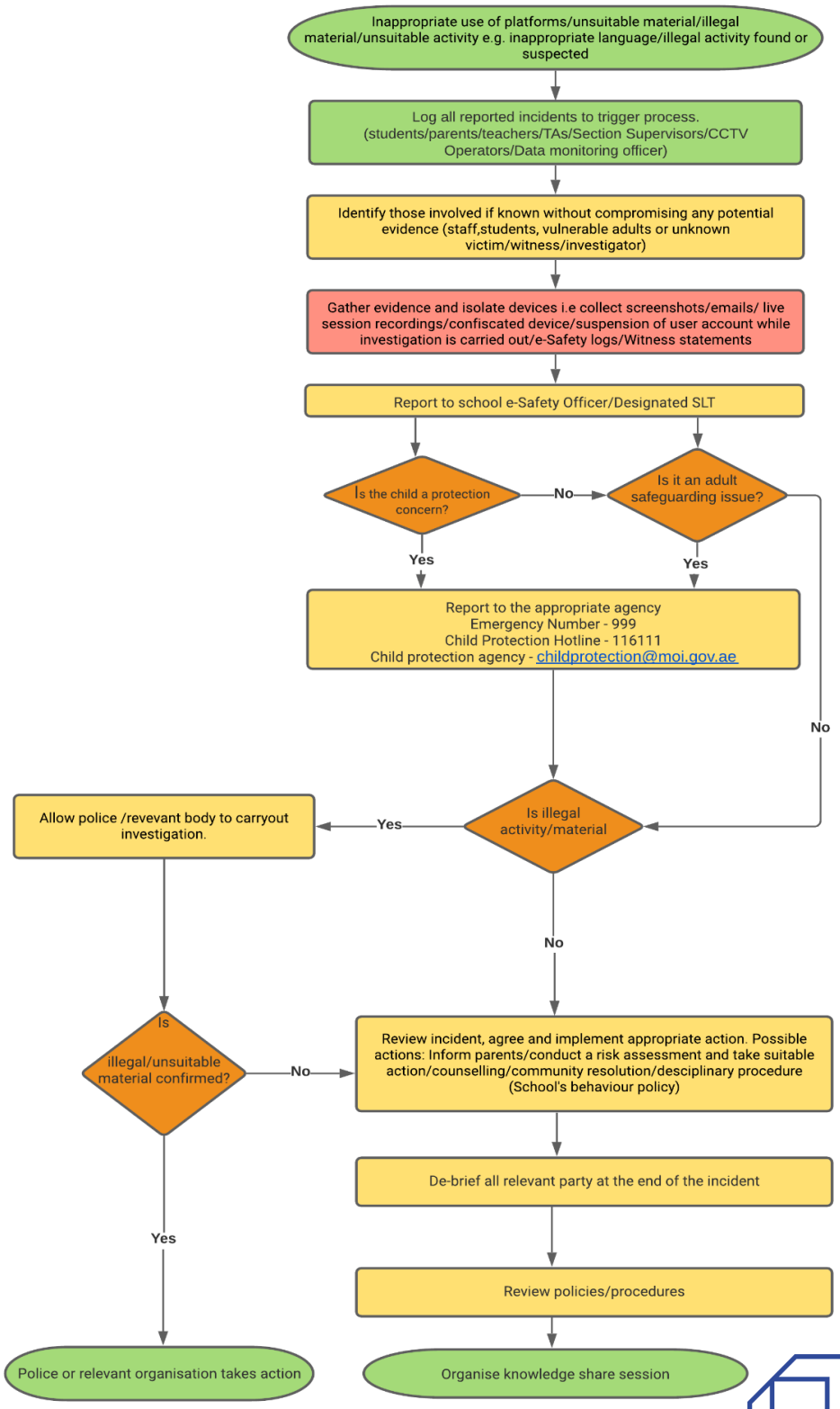
- لا يتم منح الضيوف حق الوصول إلى نظام المدارس (أي الملفات والمجلدات).
- يتم إصدارها بكلمة مرور WiFi مؤقتة للوصول إلى الإنترنت.
- جميع مجموعات المستخدمين ؛ الطلاب والموظفين والضيوف لديهم SSID منفصل.

العقوبات

سيضمن المدير ، عبر مسؤول السلامة الإلكترونية ، التعامل مع أي إساءة استخدام أو حادث بشكل مناسب ، وفقًا لسياسة السلوك بالمدرسة ، واتخاذ الإجراء المناسب.

- تشمل العقوبات التي سيتم تطبيقها حسب الاقتضاء: تعليق وصول الفرد إلى الإنترنت في المدرسة و / أو تعليق حساب المستخدم الخاص بالفرد لفترة من الوقت.
- في الحالات الخطيرة (وحيث يستمر التنمر الإلكتروني من قبل فرد ما) ، قد يقرر المدير استبعاد الشخص أو الأشخاص المسؤولين من المدرسة.
- من خلال التواصل المنتظم بين مسؤول السلامة الإلكترونية والأخصائيين الاجتماعيين والمدرسين ، من المأمول أن يتم التعرف بسرعة على أي تلميذ يبدو أنه ضحية للتنمر عبر الإنترنت أو يتعرض للتنمر عبر الإنترنت بشكل متكرر.
- عندما يرى الأخصائي الاجتماعي أن ذلك ضروريًا ، ستكون هناك حاجة إلى حسابات مكتوبة من جميع المعنيين. يقوم الأخصائي الاجتماعي بالاتصال بوالدي التلاميذ المعنيين.
- في حالة وجود حادثة تنمر عبر الإنترنت ، أو غيرها من حوادث السلامة الإلكترونية التي تغطيها هذه السياسة ، والتي قد تحدث خارج المدرسة ، ولكنها مرتبطة بعضوية المدرسة ، يمكن للمدير أن يفرض عقوبات تأديبية على السلوك غير المناسب عندما يكون ذلك معقولًا .
- ستتعامل المدرسة مع مثل هذه الحوادث ضمن هذه السياسة والسلوكيات المرتبطة بها ومكافحة التنمر ، وستقوم ، حيثما كان معروفًا ، بإبلاغ أولياء الأمور / مقدمي الرعاية بحوادث السلوك غير الملائم للسلامة الإلكترونية التي تحدث خارج المدرسة.
- سيتم التعامل مع عدم الالتزام بالسياسة وفقًا لسياسة سلوك المدرسة بالكامل وسياسة حماية الطفل في المدرسة.

إجراءات الإبلاغ عن حادثة السلامة الإلكترونية



مراجعة السياسة وتحديثها

المؤلفون :	Liwa Schools - E-Safety Audit Committee
تكرار المراجعة:	Quarterly
تاريخ المراجعة:	1st April 2021
تاريخ المراجعة التالية:	1st July 2021