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

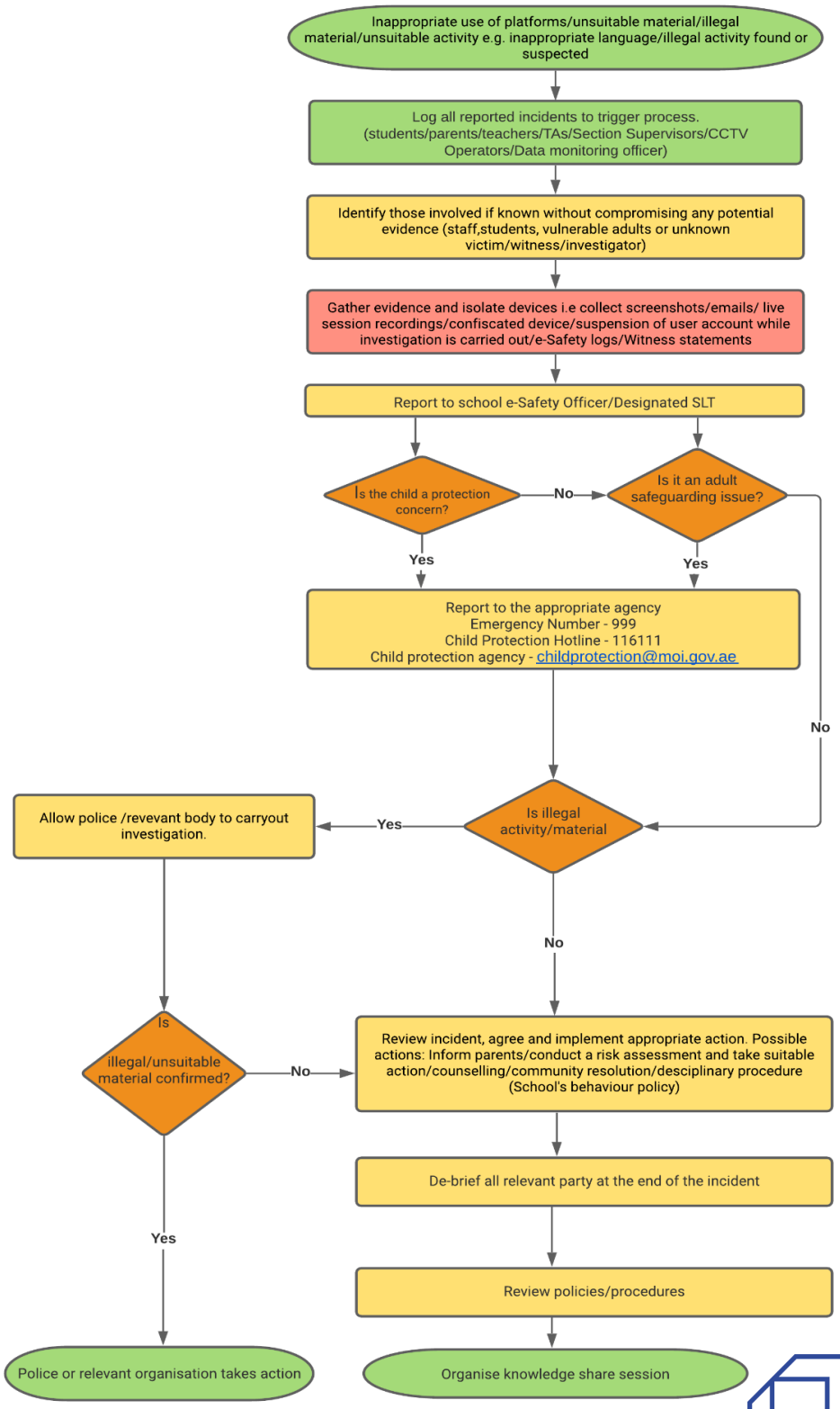
- لا يتم منح الضيوف حق الوصول إلى نظام المدارس (أي الملفات والمجلدات).
- يتم إصدارها بكلمة مرور WiFi مؤقتة للوصول إلى الإنترنت.
- جميع مجموعات المستخدمين ؛ الطلاب والموظفين والضيوف لديهم SSID منفصل.

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:	Annual
تاريخ المراجعة:	1st August 2021
تاريخ المراجعة التالية:	1st August 2022

E-Safety Policy

Policy Statement

Rationale

It is the duty of the school to ensure that children and young people are protected from potential harm both within the school and beyond. The e-safety policy applies to all members of the school community and is to be adhered to by all (including staff, students / pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of the school's ICT systems, both in and out of school. Should there be an incident of cyber bullying, or other e-safety incidents covered by this policy, which may take place out of school, but is linked to membership of the school, the school will impose disciplinary penalties for inappropriate behaviour where this is reasonable as stipulated in the school's behavior policy.

The school will deal with such incidents within this policy and associated behaviours and will, where known, inform parents / carers of incidents of inappropriate e-safety behaviour that takes place out of school.

Aims

- To emphasise the need to educate staff, children and young people about the pros and cons of using new technologies both within and outside school.
- To provide safeguards and agreement for acceptable use to guide all users, whether staff or student, in their online experiences.
- To ensure adults are clear about procedures for misuse of any technologies both within and beyond the school.
- To develop links with parents/carers and the wider community ensuring their input into policies and procedures with continued awareness of the benefits and potential issues related to technologies.

Definitions

The term 'e-safety' is used to encompass the safe use of all technologies in order to protect children, young people and adults from potential and known risks.

Designated Roles and Procedures

Governors and Principals

It is the overall responsibility of the Principals to ensure the Governors understand their responsibility and to have an overview of e-Safety as part of the wider remit of safeguarding across the school with further responsibilities as follows:

- The Principal has designated an e-Safety officer to implement agreed policies, procedures, staff training, curriculum requirements and to take responsibility for ensuring e-Safety is addressed in order to establish a safe ICT learning environment. All staff and students are aware of the person who has been appointed to this role within the school.
- There is a standard disclaimer on all emails stating that the views expressed are not necessarily those of the school or organisation.
- Resources should be provided for the e-Safety officer to be trained with up to date information in order for them to update policies, where appropriate.
- All staff are responsible for promoting e-Safety across the curriculum.

E-Safety Officer

It is the role of the designated e-Safety officer to:

- ❏ Promote the importance of e-safety within school as part of its duty of care to ensure the safety of their pupils and staff.
- ❏ Establish and maintain a safe ICT learning environment within the school.
- ❏ Ensure that the Acceptable Use Agreements are reviewed annually, with up-to-date information, and that training is available for staff to teach e-Safety and for parents to feel informed and know where to go for advice.
- ❏ Work alongside the Network Manager to ensure that filtering is set to the correct level for staff, children and young people.
- ❏ Equip (i.e. training) children to stay safe online, both in school and outside of school.
- ❏ Ensure that all adults are aware of the filtering levels and why they are there to protect children and young people.
- ❏ Liaise with the Cyber Safety PLC to discuss and mitigate e-Safety trends or threats identified within the school so that policies and procedures are up-to-date to take account of any emerging issues and technologies.

- ❏ Update staff about new and emerging technologies so that the correct e-safety information can be taught or adhered to.
- ❏ Oversee transparent monitoring of the Internet and online technologies. The school's Internet firewall system also provides a high level of transparent monitoring as part of its functionality.
- ❏ Regularly analyse the e-Safety incident logs to help inform future development and safeguarding, where risks can be identified.
- ❏ Work alongside the Network Manager to ensure there is appropriate and up-to-date anti-virus software and anti-spyware on the network, stand-a-lone PCs and teacher/child laptops and that this is reviewed and updated on a regular basis.
- ❏ Ensure that unsolicited emails to a member of staff from other sources is minimised.
- ❏ Advise on the e-Safety curriculum review to ensure it is up-to-date to take account of any emerging issues and technologies.
- ❏ Provide regular reports to the Senior Leadership Team.

E-Safety Officer - Job Description

- ❏ Developing an e-safety culture under the direction of the management team and acting as a named point of contact on all e-safety issues.
- ❏ Ensuring that everyone including children and young people know what to do if they are concerned about an e-safety issue.
- ❏ Ensuring that e-safety is embedded within continuing professional development (CPD) for staff and co-ordinating training as appropriate.
- ❏ Ensuring that e-safety is embedded across the curriculum and in all concerned activities as appropriate.
- ❏ Ensuring that e-safety is promoted to parents and carers, other users of ICT within the Liwa community.
- ❏ Ensuring that adequate resources are provided to all pupils to support them in their understanding of all issues concerning e-safety..
- ❏ Maintaining an e-safety incident log.
- ❏ Monitoring and reporting on e-safety issues to the management team, and other agencies as appropriate.
- ❏ Developing an understanding of the relevant local and national guidance.
- ❏ In consultation with the SLT, liaising with the local authorities as appropriate.
- ❏ Reviewing and updating e-safety policies and procedures on a regular basis and after an incident.
- ❏ Ensure that learning outcomes and feedback are appropriately shared.
- ❏

- ❏ Ensuring that the infrastructure and technology provides a safe and secure environment for all within the Liwa community.
- ❏ Ensure that the school has Firewalls.
    - ❏ Anti-virus and anti-spyware software.
    - ❏ Filters.
    - ❏ Awareness of any wireless technology issues.
    - ❏ A clear policy on using personal devices.

Cyber Safety Professional Learning Committee.

It is the responsibility of the committee within the school to:

- ❏ Review all policies and protocols pertaining to E-Safety.
- ❏ Ensure all the school has an E-Safety training programme
- ❏ Ensure teachers implement cyber safety lessons into their ongoing lessons.
- ❏ Ensure the school environment is safe and secure and that appropriate safety protocols are in place.
- ❏ Plan regular community events related to e-safety.

Data Protection Officer

It is the role of the designated e-Safety officer to:

- ❏ Providing training on compliance requirements
- ❏ Provide training to staff involved in data processing
- ❏ Conducting audits to ensure compliance and address potential issues proactively
- ❏ Serving as the point of contact between the school and the regulatory authorities.
- ❏ Monitoring performance and providing advice on the impact of data protection efforts
- ❏ Maintaining comprehensive records of all data processing activities conducted by the school, including the purposes of all processing activities, which must be made public on request
- ❏ Interfacing with data subjects to inform them about how their data is being used, their right to have their personal data erased, and what measures the company has put in place to protect their personal information.

Data Protection : Job Description

- ❏ An understanding of the Data Protection Law (contents and interpretation) and how this is applied and aligned to the school's data protection policy.
- ❏ Interpreting regulatory requirements and providing advice on how this could be applied within the school.

- ❏ Liaising with external counterparts (regulators) as well as internal stakeholders to support in the implementation of the school's data protection policy in compliance to the UAE law.
- ❏ Provide data protection awareness staff training to all stakeholders.

E-Safety Data Monitoring Officer

It is the role of the designated e-Safety officer to:

- ❏ Establish and coordinate the e-safety monitoring system including data collection, analysis and review.
- ❏ Identify appropriate e-safety infringement indicators, how these are monitored and reviewed.
- ❏ Work closely with the relevant teams (Network Administrator, E-learning Co-ordinators and Device management team) to prepare specific data collection methods and tools
- ❏ Coordinate monitoring activities and inputs required of other team members.
- ❏ Anticipate, plan and support reporting requirements.
- ❏ Ensure information gathered through monitoring activities is shared quickly and in an appropriate format with the E-Safety Officer so that any problems arising can be addressed.

Staff and Adults

It is the responsibility of all adults within the school to:

- ❏ Check that the filtering levels are appropriate for pupils and are set at the correct level and to report any concerns to the e-Safety officer.
- ❏ Alert the e-Safety officer of any new or arising issues and risks that may need to be included within policies and procedures.
- ❏ Ensure that all pupils are protected and supported in their use of technologies so that they know how to use them in a safe and responsible manner. All pupils should know what to do in the event of an incident.
- ❏ Be up-to-date with e-Safety knowledge that is appropriate for the age group and reinforce through the curriculum.
- ❏ Report accidental access to inappropriate materials to the e-Safety officer in order that inappropriate sites are added to the restricted list.
- ❏ Use anti-virus software and check for viruses on their work laptop, memory stick or a CD ROM when transferring information from the internet on a regular basis, especially when not connected to the school/education setting or other establishment's network.

- ❏ Ensure that all sensitive information is only stored on the school's network and can only be accessed by authenticated users within the school domain as stated in the data protection policy. (No sensitive data should be saved on local drives or personal storage devices.)
- ❏ Report incidents of personally directed "bullying" or other inappropriate behavior via the Internet or other technologies to the e-Safety officer.
- ❏ Be aware that by submitting the school policy's online form you are agreeing to be bound by the terms of the policy.
- ❏ Be aware of e-safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school policies with regard to these devices.
- ❏ In lessons, where internet use is pre-planned, students / pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.

Pupils

It is the responsibility of all pupils within the school to:

- ❏ Be responsible users of the school ICT systems in accordance with the school's Acceptable Use Policy.
- ❏ To understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
- ❏ To understand the school policies on the use of mobile phones, digital cameras and hand-held devices. (policies on the taking / use of images and on cyber-bullying.
- ❏ Adopt good e-safety practice when using digital technologies out of school and realize that the school's E-Safety Policy covers their actions out of school, if related to their membership of the school.
- ❏ Have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.

Guests/Visitors

It is the responsibility of all guests within the school to:

- ❏ Understand that Guests are not given access to the school systems except WiFi.
- ❏ Use the school's systems and devices, including its wireless network, in a responsible way, to ensure that there is no risk to Pupils' safety or to the safety and security of the systems, devices and other users.
- ❏ Report accidental access to inappropriate materials to the e-Safety officer in order that inappropriate sites are added to the restricted list.

Operational Implementation

Education - All Students

Whilst regulation and technical solutions are very important, their use must be balanced by educating all students to take a responsible approach. Therefore, the education of students and their carers in e-safety is an essential part of our e-safety provision.

E-Safety education will be provided in the following ways:

- A planned e-safety program is provided as part of the ICT curriculum and through PACE (Personal and Community Education).
- The curriculum is regularly re-visited to cover both the use of ICT and new technologies in school and outside school. Key e-safety messages are reinforced as part of a planned program of assemblies and tutorial / pastoral activities.
- Students are taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information.
- Students are encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside school.
- Students are taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
- Rules for use of ICT systems / internet are posted in all rooms.
- Staff are required to act as good role models in their use of ICT, the internet and mobile devices.

Education & Staff Training

It is essential that our staff receive e-safety training and understand their responsibilities, as outlined in this policy:

- E-safety training for staff is provided as part of our induction program at the beginning of the school year and throughout the course of the year as required.
- All staff are regularly updated with relevant e-safety developments
- This E-Safety policy is presented to and discussed by staff in staff / team meetings / INSET days.
- The E-Safety Officer will provide advice / guidance / training to individuals as required.

Education - Liwa Community

We value the contribution that the wider community makes in ensuring that our students are safe, as such we will continue to support the wider Liwa community in all matters relating to e-safety.

- ❏ Regular updates will be provided to parents on current e-safety threats and how they may protect themselves and their families.
- ❏ Basic e-safety training will be provided on how to secure accounts and set/check privacy settings.
- ❏ Regular updates/reminders on how to report any issues/concerns regarding e-safety in the school.
- ❏ Advice on how to monitor or manage what their children are doing online including managing screen time.

The Curriculum

- ❏ Cyber security and ethics is a key component of the ICT curriculum for all Grades (K-12), key competencies covered ensure progression across the grades and are aligned to expected grade outcomes.
- ❏ E-safety is a focus in all areas of the curriculum and staff should reinforce e-safety messages in the use of technology across the curriculum.
- ❏ In lessons, where internet use is pre-planned, it is best practice that students should be guided to sites checked as suitable for their use.
- ❏ Most sites are blocked by default by the Network filtering and a request must be made by the teachers so that access is given to the students. All sites are examined before permission is granted.
- ❏ Where students can freely search the internet, e.g. using search engines, staff should be vigilant in monitoring the content of the websites young people visit.
- ❏ Students should be taught in all lessons, to be critically aware of the materials / content they access online and be guided to validate the accuracy of information
- ❏ Students should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.

Password Policy Implementation

Staff and Students' Passwords

1. All users are issued with a **temporary password when the email is initially created and shared.**
2. Emails currently created for all students Grades 3-12 and staff.
3. Once the account is created, **users are immediately asked to change their password.**

4. The recommended strength and accepted criteria for the password is suggested by the system; **passwords that do not meet the criteria are not accepted.**
5. In the case of a forgotten password or a need to reset the password if this has been compromised then a **request for a password reset by the parents to the school** using the school's communication channels is sent to request the reset. The new password is then shared with the parent that has requested the reset.
6. Staff can request the information directly from the IT team by calling them on the school's support telephone number.
7. **The password refresh will be applied twice a year for all students Grade 3-12 and every 90 days for staff.**
8. **All passwords for KG-Grade 2 students** will be set once a year and all passwords will be communicated to the parents by the class teacher via ClassDojo.
9. No database of the staff or students passwords are available, IT support only has the reset option.

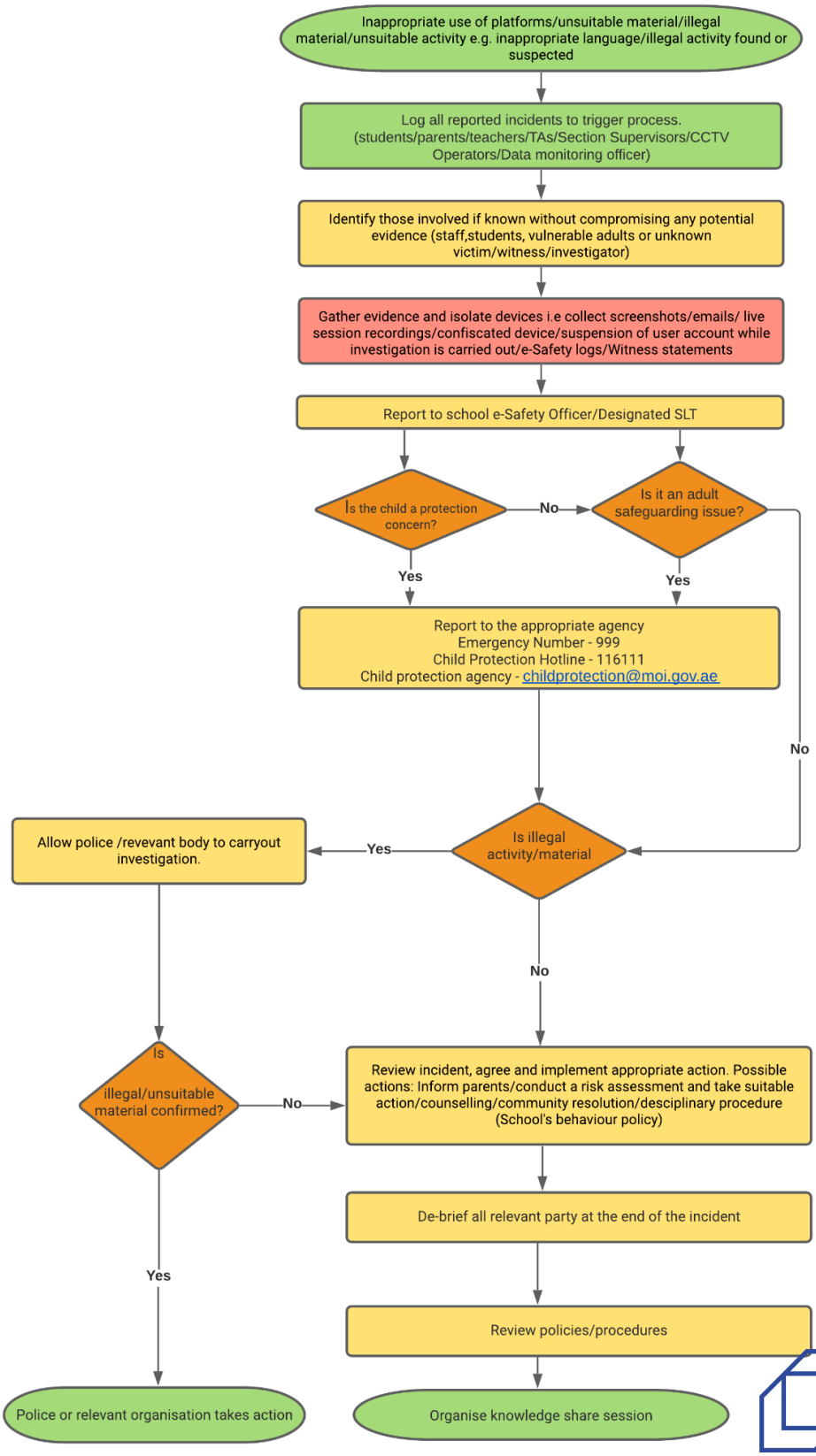
Guest/ Visitor's Access

1. Guests are not given access to the school's system (i.e. files and folders).
2. They are issued with a **temporary WiFi password** for internet access.
3. All user groups; students, staff and guests have a **separate SSID**.

Sanctions

1. The Principal, via the e-safety officer, will ensure that any misuse or incident has been dealt with appropriately, according to the school's behavior policy, and that appropriate action is taken.
2. Sanctions to be applied as appropriate include: suspension of an individual's internet access at School and/or suspension of an individual's user account for a period of time.
3. In serious cases (and where cyberbullying by an individual continues) the Principal may decide to exclude from School the person or persons responsible.
4. Through regular communication between the e-safety officer, social workers and teachers, it is hoped that any pupil who either seems to be a victim of cyberbullying or is repeatedly being a cyberbully will be quickly identified.
5. When it is deemed necessary, by the social worker, written accounts will be required from all those involved. The social worker will contact the parents of those pupils involved.
6. Should there be an incident of cyber bullying, or other e-safety incidents covered by this policy, which may take place out of school, but is linked to membership of the school, the Principal can impose disciplinary penalties for inappropriate behavior where this is reasonable.
7. The school will deal with such incidents within this policy and associated behaviors and anti-bullying and will, where known, inform parents / carers of incidents of inappropriate e-safety behavior that takes place out of school.
8. Failure to adhere to the policy will be dealt with in accordance with the school's Rewards and Sanctions Policy, the School's Code of Conduct and when necessary the Child Protection Policy.

E-Safety Incident Report Procedure



Appendix

Federal Law No. 5 of 1985: The Civil Code

Federal Law No. 3 of 1987: The Penal Code ('the Penal Code')

Policy Review and Update

Author(s):	Liwa Schools - E-Safety Audit Committee
Review frequency:	Annual
Review Date:	1st August 2021
Date of Next Review:	1st August 2022