سياسة السلامة الإلكترونية
وثيقة السياسة

سبتمبر 2023

Policy Reference	ET-04-Ar
Version	V1
Date of Draft	10 October 23
Policy Owner	Director of ET
Date of Approval	12102023
Effective Date	16102023
Date of Review	12102026
Reviewed by	Deputy CEO
Approved by	CEO

ليـــوا للتعليم
Liwa Education

ليـــوا للتعليم
Liwa Education

بيان السياسة

تحرص المدرسة على تعزيز السلامة الإلكترونية كونها جزءاً هاماً للغاية في الحفاظ على سلامة الطلاب وحمايتهم من أي مخاطر أو تهديدات قد يتعرضون لها داخل وخارج المدرسة. وتنطبق سياسة السلامة الإلكترونية على جميع أعضاء المجتمع المدرسي. وبالتالي يتعين على الجميع، ممن يستخدمون أنظمة تكنولوجيا المعلومات والاتصالات الخاصة بالمدرسة داخلها وخارجها (العاملين بالمدرسة والطلاب والمتطوعين وأولياء الأمور والزوار والعملاء) الإلتزام بتطبيق كل ما هو منصوص عليه في هذه السياسة. وفي حال وقوع حادثة التنمر الإلكتروني أو أياً من حوادث السلامة الإلكترونية المدرجة في هذه السياسة والتي قد تحدث خارج المدرسة، إلا أنها مرتبطة بعضوية المدرسة، يحتم على إدارة المدرسة القيام بفرض عقوبات تأديبية على مخالفي قواعد السلوك الإيجابي وفقاً لما هو منصوص عليه في لائحة السلوك الطلابي.

وتقوم إدارة المدرسة بتطبيق الإجراءات المنصوص عليها في هذه السياسة عند وقوع مثل هذه الحوادث وما يرتبط بها من سلوكيات، حيث يتم القيام بإبلاغ أولياء الأمور / مقدمي الرعاية بالسلوكيات المخالفة لقواعد السلامة الإلكترونية والتي تحدث خارج المدرسة.

الغرض

- التأكيد على ضرورة توعية كلاً من الإداريين والمعلمين والأطفال والشباب بإيجابيات وسلبيات استخدام وسائل التكنولوجيا الحديثة داخل المدرسة وخارجها.
- تطبيق سياسة الاستخدام المقبول للإنترنت بهدف التأكد من أن جميع الموظفين والطلاب على دراية تامة بمخاطرإستخدام الإنترنت بما يضمن إستخدامه بشكل مسؤول وآمن.
- التأكد من أن البالغين على دراية تامة بالإجراءات والعقوبات التي سيتم اتخاذها حال سوء إستخدام الأجهزة الإلكترونية ووسائل التكنولوجيا الحديثة داخل المدرسة وخارجها.
- إشراك أولياء الأمورعلى نطاق واسع في مختلف جوانب الحياة المدرسية بما يضمن مساهمتهم في السياسات والإجراءات مع الإستمرار في توعيتهم بإيجابيات وسلبيات التكنولوجيا الحديثة.

التعريفات

السلامة الإلكترونية: هي الإستخدام الآمن لجميع موارد تقنية المعلومات بهدف حماية الأطفال والشباب من المخاطر المحتملة والمعروفة.

الأدوار والمسؤوليات

المُدراء وأعضاء فريق القيادة العليا

يقع على عاتق المدراء مسؤولية التأكد من أن أعضاء فريق القيادة العليا على دراية بأدوارهم ومهامهم وأن يكونوا على وعي تام بكل ما هو متعلق بالسلامة الإلكترونية وأهميتها في حماية جميع أفراد المجتمع المدرسي مع المزيد من المسؤوليات على النحو التالي:

- قيام مدير المدرسة بتعيين مسؤول للأمن الإلكتروني لتنفيذ السياسات والإجراءات المتفق عليها وإعطاء الدورات التدريبية للمعلمين فيما يخص الاستخدام الآمن لأنظمة التكنولوجيا المعلومات والإتصالات وما تتطلبه المناهج الدراسية وتحمل مسؤولية

توفير بيئة تعليمية آمنة إلكترونياً. والتأكيد على أن جميع الإداريين والمعلمين والطلاب على دراية بالشخص الذي تم تعيينه لهذا الدور بالمدرسة.

- القيام بإضافة نص إخلاء المسؤولية في جميع رسائل البريد الإلكتروني والتي تنص على أن الآراء المعبرعنها في البريد الإلكتروني لا تمثل بالضرورة آراء المدرسة أو المؤسسة.
- توفير المصادر اللازمة لمسؤول الأمن الإلكتروني من أجل تزويده بجميع المعلومات والمستجدات الخاصة بالسلامة الإلكترونية مما يؤهله من تحديث السياسات عند الضرورة.
- يتحمل المعلمين مسؤولية تعزيز السلامة الإلكترونية عبر المناهج الدراسية.

مسؤول الأمن الإلكتروني (الأدوار والمسؤوليات):

- إن أحد واجبات مسؤول الأمن الإلكتروني هو تعزيز السلامة الإلكترونية داخل المدرسة لضمان حماية الإداريين والمعلمين والطلاب من أي مخاطر أو محتوى غير لائق.
- إنشاء بيئة تعليمية آمنة إلكترونياً داخل المدرسة والحفاظ عليها من وقوع أي جرائم إلكترونية.
- التأكد من مراجعة سياسات الإستخدام المقبول لموارد تقنية المعلومات سنوياً وأن يتم تحديثها باستمرار مع ضرورة القيام بإعطاء الإداريين والمعلمين وأولياء الأمور ورش تدريبية حول السلامة الإلكترونية من أجل توعيتهم بمخاطر استخدام الإنترنت ومعرفة إلى أين يتوجهون للحصول على النصيحة والدعم عند تعرضهم لأي أذى أو تهديد عبر الإنترنت.
- العمل جنباً إلى جنب مع مدير الشبكة لضمان ضبط تصفية المحتويات على المستوى الصحيح للإداريين والمعلمين والأطفال والشباب.
- القيام بإعطاء ورش تدريبية للأطفال حول السلامة الإلكترونية من أجل ضمان حمايتهم من التعرض لأي مخاطر أو تهديدات عبر الإنترنت داخل المدرسة وخارجها.
- التأكد من أن جميع البالغين على دراية بمستويات تصفية المحتوى وأسباب توافرها بهدف حماية الأطفال والشباب من التعرض لأي محتوى غير لائق أو مُنافي للقيم الأخلاقية.
- التواصل مع لجنة التعليم المهني للأمن الإلكتروني لمناقشة كل ما هو متعلق بالسلامة الإلكترونية بما فيها التهديدات والمخاطر التي يتعرض لها الطلاب والإداريين والمعلمين داخل المدرسة مع القيام بتحديث السياسات والإجراءات بناءاً على المستجدات والتحديات التي يواجهها أفراد المجتمع المدرسي في مجال الأمن الإلكتروني.
- القيام بتعريف جميع الإداريين والمعلمين بوسائل التكنولوجيا الحديثة والناشئة وبالتالي ضمان معرفتهم بالمبادئ الصحيحة للسلامة الإلكترونية والإلتزام بها.
- القيام بالإشراف والرقابة على مواقع الإنترنت. وفي هذا الإطار، يوفر نظام جدار الحماية على شبكة الإنترنت مستوى عالي من المراقبة الشفافة كجزء من وظائفه.
- القيام بتحليل سجلات الجرائم الإلكترونية على نحو منتظم من أجل المساعدة في فرض إجراءات للحد من هذه الجرائم وإستحداث أساليب جديدة لمكافحتها بشكل فعال في المستقبل.

- العمل جنباً إلى جنب مع مدير الشبكة للتأكد من وجود برامج مناسبة وحديثة لمكافحة الفيروسات والتجسس على شبكة الإنترنت وأجهزة الكمبيوتر الشخصية وأجهزة الكمبيوتر المحمولة الخاصة بالمعلمين والطلاب وأن يتم مراجعتها وتحديثها بشكل منتظم.
- التأكد من تقليل رسائل البريد الإلكتروني الغيرمرغوب فيها والتي يتم إرسالها إلى أحد الإداريين أو المعلمين من مصادر أخرى.
- تقديم المشورة بشأن مراجعة سياسات السلامة الإلكترونية وتحديثها بإستمرار وفقاً للتطورات والمستجدات فيما يتعلق بالتقنيات الحديثة والمخاطر والتحديات.
- القيام بتقديم تقارير منتظمة إلى فريق القيادة العليا.

مسؤول الأمن الإلكتروني (الوصف الوظيفي):

- الإرتقاء بمستوى ثقافة السلامة الإلكترونية تحت إشراف فريق الإدارة والعمل كنقطة إتصال محددة للبحث في جميع القضايا التي تتعلق بالسلامة الإلكترونية.
- التأكد من أن جميع الأفراد بما في ذلك الأطفال والشباب على دراية تامة بالإجراءات الواجب إتخاذها حال تعرضهم لحوادث السلامة الإلكترونية.
- التأكد من إدراج السلامة الإلكترونية ضمن برامج التطوير المهني المستمر مع القيام بتنظيم ورش تدريبية تثقيفية للمعلمين والإداريين بشأن السلامة الإلكترونية حسب الإقتضاء.
- التأكد من تضمين السلامة الإلكترونية في المناهج الدراسية والأنشطة المعنية حسب الإقتضاء.
- التأكد من تعزيز ثقافة السلامة الإلكترونية لأولياء الأمور وجميع المستخدمين وتعريفهم بالممارسات الصحيحة للإستخدام الآمن لوسائل تكنولوجيا المعلومات والإتصالات للحماية من مخاطر الإنترنت وذلك على مستوى مدارس ليوا الثلاث.
- التأكد من توفير المصادر الكافية لجميع الطلاب من أجل دعمهم لفهم جميع القضايا المتعلقة بالسلامة الإلكترونية.
- الإحتفاظ بسجل خاص بحوادث السلامة الإلكترونية.
- المراقبة الدورية لحوادث السلامة الإلكترونية والإبلاغ عنها لفريق الإدارة وتصعيدها للجهات المختصة إذا لزم الأمر.
- تعزيز الفهم للإرشادات المحلية والوطنية لكل ما هو متعلق بالسلامة الإلكترونية.
- التشاور مع أعضاء فريق القيادة العليا بشأن التنسيق مع السلطات المحلية حسب الإقتضاء.
- القيام بمراجعة وتحديث سياسات وإجراءات السلامة الإلكترونية على نحو منتظم وعند ظهور حوادث أو جرائم إلكترونية.
- التأكد من مشاركة نواتج التعلم والملاحظات بشكل لائق بحيث لا يتضمن أية ألفاظ بذيئة أو إهانات.
- التأكد من أن البنية التحتية لتكونولجيا المعلومات والإتصالات قادرة على توفير بيئة آمنة إلكترونياً لجميع الأفراد على مستوى مدارس ليوا الثلاث.

- التأكد من توفر جدران الحماية لشبكة الإنترنت بالمدرسة.
- التأكد من توفر برامج لمكافحة الفيروسات والتجسس.
- التأكد من توفر المرشحات.
- الوعي بالقضايا التي تتعلق بالتقنية اللاسلكية.
- التأكد من اعتماد سياسة واضحة لاستخدام الأجهزة الإلكترونية الشخصية.

لجنة التعلم المهني للسلامة الإلكترونية (الأدوار والمسؤوليات):

- القيام بمراجعة جميع السياسات والبروتوكولات المتعلقة بالسلامة الإلكترونية.
- التأكد من أن المدارس لديها برنامج تدريبي للسلامة الإلكترونية.
- التأكد من قيام المعلمين بتضمين مواضيع السلامة الإلكترونية في المناهج والمقررات الدراسية على نحو مستمر.
- التأكد من أن بيئة المدرسة آمنة إلكترونياً وأنه يتم تطبيق جميع سياسات وبروتوكولات السلامة الإلكترونية.
- التخطيط لتنظيم فعاليات مجتمعية تتعلق بالسلامة الإلكترونية.

مسؤول حماية البيانات (الأدوار والمسؤوليات):

- القيام بإعطاء ورش تدريبية على متطلبات الإمتثال.
- القيام بإعطاء ورش تدريبية للموظفين المشاركين في معالجة البيانات.
- القيام بإجراء عمليات تدقيق لضمان الإمتثال والمعالجة الإستباقية للقضايا المحتملة.
- العمل كنقطة إتصال بين المدرسة والسلطات التنظيمية.
- القيام بمراقبة الأداء وتقديم المشورة بشأن تأثير جهود حماية البيانات.
- الإحتفاظ بسجلات شاملة لجميع أنشطة معالجة البيانات التي تجريها المدرسة بما في ذلك أغراض جميع أنشطة المعالجة والتي يجب إتاحتها للاشخاص المعنيين عند الطلب.
- القيام بالتواصل مع موضوعات البيانات لإبلاغهم بكيفية إستخدام بياناتهم وحقهم في محو بياناتهم الشخصية وما هي الإجراءات التي اتخذتها المؤسسة لحماية بياناتهم الشخصية.

مسؤول 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.

- التنسيق مع النظراء الخارجيين (المنظمين) وكذلك أصحاب المصلحة الداخليين لدعم تطبيق سياسة حماية البيانات للمدرسة بما يتماشى مع قانون دولة الإمارات العربية المتحدة.
- القيام بإعطاء ورش تدريبية للموظفين للتوعية بشأن حماية البيانات الشخصية لجميع أصحاب المصلحة.

مسؤول مراقبة بيانات السلامة الإلكترونية (الأدوار والمسؤوليات):

- القيام بإنشاء وتنسيق نظام مراقبة السلامة الإلكترونية بما في ذلك جمع البيانات وتحليلها ومراجعتها.
- القيام بتحديد المؤشرات المناسبة بشأن التعدي على السلامة الإلكترونية وكيفية مراقبتها ومراجعتها.
- العمل عن كثب مع الفرق المعنية (مسؤول الشبكة ومنسقي التعلم الإلكتروني وفريق إدارة الأجهزة) لإعداد طرق وأدوات محددة لجمع البيانات.
- القيام بتنسيق رصد الأنشطة والمدخلات المطلوبة من أعضاء الفريق الآخرين.
- التوقع والتخطيط ودعم لمتطلبات إعداد التقارير.
- التأكد من سرعة مشاركة المعلومات التي تم جمعها من خلال أنشطة المراقبة وبشكل مناسب مع مسؤول الأمن الإلكتروني بحيث يمكن معالجة أية مشاكل قد تحدث.

الإداريين والمعلمين والبالغين (الأدوار والمسؤوليات):

- التحقق من أن مستويات التصفية مناسبة للطلاب وأنها مضبوطة على المستوى الصحيح مع القيام بإبلاغ مسؤول الأمن الإلكتروني بأية شكاوى أو ملاحظات.
- القيام بتنبيه مسؤول الأمن الإلكتروني من أية تهديدات أو مخاطر جديدة قد تحتاج إلى إدراجها في السياسات والإجراءات.
- الإطلاع الدائم على آليات تعزيز السلامة الإلكترونية المناسبة للفئة العمرية وتضمينها في المناهج الدراسية.
- القيام بإبلاغ مسؤول الأمن الإلكتروني عن الوصول الغير مقصود للمواقع ذات المحتوى الغير لائق أو المسيء من أجل إضافتها في القائمة الخاصة بوضع تقييد المحتوى.
- القيام بإستخدام برنامج مكافحة الفيروسات من أجل فحص الفيروسات على أجهزة الكمبيوتر المحمول الخاصة بالعمل أو بطاقة الذاكرة أو القرص المضغوط وذلك عند نقل البيانات من الإنترنت على نحو منتظم ، خاصةً عندما لا تكون متصلة بإعدادات المدرسة أو بشبكة مؤسسة أخرى.
- التأكد من تخزين جميع المعلومات الحساسة فقط على شبكة المدرسة ولا يمكن الوصول إليها إلا من قبل المستخدمين المصادق عليهم داخل نطاق المدرسة كما هو منصوص عليه في سياسة حماية البيانات. (يجب عدم حفظ أي بيانات حساسة على محركات الأقراص المحلية أو أجهزة التخزين الشخصية).
- القيام بإبلاغ مسؤول الأمن الإلكتروني عن حوادث التنمر الإلكتروني أو أية سلوكيات غير لائقة عبر الإنترنت ووسائل التكنولوجيا الأخرى.

- الدراية التامة أنه في حال تعبئة وتسليم نموذج سياسة المدرسة عبر الإنترنت، فإنه إقرار بالموافقة على جميع البنود الواردة في السياسة.
- الإلمام بقضايا السلامة الإلكترونية التي تتعلق بإستخدام الهواتف المحمولة والكاميرات والأجهزة المحمولة باليد وأنه يتم مراقبة إستخدام هذه الأجهزة بالإضافة إلى تطبيق سياسة المدرسة الحالية فيما يتعلق بهذه الأجهزة.
- وفي الحصص الدراسية، حيث يكون إستخدام الإنترنت مخططاً بشكل مسبق، ينبغي توجيه الطلاب إلى المواقع الإلكترونية التي تم فحصها مسبقاً للتأكد من أن محتواها مناسب لإستخدامها ويتم إتباع هذه الإجراءات للتعامل مع أية مواقع إلكترونية ذات محتوى غير لائق توجد في عمليات البحث على الإنترنت.

الطلاب (الأدوار والمسؤوليات):

- العلم بأنه لا يتم منح الزوار إمكانية الوصول إلى أنظمة المدرسة بإستثناء شبكة الواي فاي WiFi
- الإستخدام المسؤول لأنظمة المدرسة وأجهزتها بما في ذلك شبكتها اللاسلكية للتأكد من عدم وجود مخاطر على سلامة الطلاب أو على سلامة وأمن الأنظمة والأجهزة والمستخدمين الآخرين.
- القيام بإبلاغ مسؤول الأمن الإلكتروني عن الوصول الغير مقصود للمواقع ذات المحتوى الغير لائق أو المسيء من أجل إضافتها في القائمة الخاصة بوضع تقييد المحتوى.

التنفيذ التشغيلي:

التعليم - جميع الطلاب

بالرغم من أن الحلول التنظيمية والتقنية مهمة جداً، إلا أنه يجب أن يكون إستخدامها متوازناً من خلال توعية وتثقيف جميع الطلاب لإنتهاج الإستخدام المسؤول لأنظمة تكنولوجيا المعلومات والإتصالات. وبالتالي فإن توعية الطلاب والقائمين على رعايتهم بآليات السلامة الإلكترونية يعد جزءاً أساسياً وهاماً لتوفير بيئة آمنة رقمياً لجميع أفراد المجتمع المدرسي.

<u>التوعية بأسس السلامة الإلكترونية عن طريق الوسائل التالية:</u>

- القيام بتوفير برنامج مخطط للسلامة الإلكترونية كجزء من المنهج الدراسي لمادة تقنية المعلومات ومن خلال التعليم الشخصي والمجتمعي.
- إعادة النظر في المنهاج الدراسي على نحو منتظم بحيث يشمل إستخدام أنظمة تكنولوجيا المعلومات والإتصالات والتقنيات الحديثة داخل وخارج المدرسة. ويتم القيام بنشر وتعزيز رسائل هامة للسلامة الإلكترونية كجزء من برنامج مخطط للتجمعات والأنشطة التعليمية والرعوية.
- توعية الطلاب بمخاطر الإنترنت بجميع الحصص الدراسية ليكونوا على دراية تامة بمحتوى المواقع الإلكترونية الذي يصلون إليه مع توجيههم للتحقق من دقة البيانات.
- حث الطلاب على تبني الإستخدام المسؤول والآمن لوسائل تكنولوجيا المعلومات والإتصالات وشبكة الإنترنت والأجهزة المحمولة داخل المدرسة وخارجها.

- يتم تعليم الطلاب التعرف على مصادر المعلومات المستخدمة وإحترام حقوق النشر عند إستخدام البيانات التي يتم الوصول إليها عبر الإنترنت.
- وضع قواعد الإستخدام الآمن لأنظمة تكنولوجيا المعلومات والإتصالات وشبكة الإنترنت بجميع الغرف.
- مطالبة الإداريين والمعلمين بأن يكونوا قدوة جيدة في إستخدامهم لأنظمة تكنولوجيا المعلومات والإتصالات وشبكة الإنترنت والأجهزة المحمولة.

التعليم وتدريب الإداريين والمعلمين:

من الضروري جداً أن يتم إعطاء ورش تدريبية للإداريين والمعلمين بشأن السلامة الإلكترونية وأن يكونوا على وعي تام بأدوارهم ومسؤولياتهم كما هو منصوص عليه في هذه السياسة كالآتي:

- القيام بإعطاء ورش تدريبية للإداريين والمعلمين بشأن السلامة الإلكترونية وذلك كجزء من البرنامج التعريفي في بداية العام الدراسي وعلى مدار العام كما هو مطلوب.
- القيام بموافاة جميع الإداريين والمعلمين على نحو منتظم بآخر التطورات والمستجدات بشأن ما هو متعلق بالسلامة الإلكترونية.
- القيام بتعريف سياسة السلامة الإلكترونية للإداريين والمعلمين ومناقشتها معهم خلال إجتماعات الإداريين والمعلمين والفريق وأيام الورش التدريبية للتطوير المهني.
- قيام مسؤول الأمن الإلكتروني بتقديم المشورة والتوجيه والإرشاد مع القيام بإعطاء الورش التدريبية للأفراد كما هو مطلوب.

التعليم - مجتمع ليوا

نحن نقدر تماماً الجهود التي يبذلها أولياء الأمور من أجل ضمان السلامة الألكترونية لأبناؤنا الطلاب، وبالتالي فإن مدارس ليوا الثلاث مستمرة في تقديم كافة أشكال الدعم لأولياء الأمور في جميع ما هو متعلق بالسلامة الإلكترونية كالآتي:

- القيام موافاة أولياء الأمور على نحو منتظم بكافة المستجدات والتطورات فيما يتعلق بقضايا السلامة الإلكترونية من تهديدات وجرائم إلكترونية و الإجراءات الواجب إتخاذها من أجل حماية أنفسهم وعائلاتهم.
- القيام بإعطاء ورشة تدريبية لأولياء الأمور حول كيفية القيام بضبط إعدادات الخصوصية.
- القيام بموافاة أولياء الأمور وتذكيرهم على نحو منتظم بالإجراءات الواجب إتخاذها من أجل الإبلاغ عن أية إساءة أو تهديدات تتعلق بالسلامة الإلكترونية في المدرسة.
- القيام بتقديم نصائح حول كيفية قيام أولياء الأمور بمراقبة سلوكيات أبنائهم عند إستخدام شبكة الإنترنت بما في ذلك إدارة وقت الشاشة.

المناهج الدراسية:

- تعد مبادئ السلامة الإلكترونية وأخلاقيات التكنولوجيا جزءاً هاماً في منهاج مادة تقنية المعلومات بجميع المراحل الدراسية (مرحلة رياض الأطفال حتى الصف الثاني عشر)، حيث أن المهارات الأساسية التي يتم تغطيتها عبر المنهاج تضمن قيام الطلاب بتحقيق مستوى التقدم الذي يتماشى مع المستوى المتوقع في المنهاج التعليمي المطبق.

- إن تضمين مبادئ وآليات السلامة الإلكترونية في جميع المناهج الدراسية يعد أمراً ضرورياً وبالتالي يتعين على جميع المعلمين القيام بتعزيز قواعد السلامة الألكترونية عند إستخدام وسائل تكنولوجيا المعلومات والإتصالات بجميع المناهج الدراسية.
- في الحصص الدراسية، حيث يكون إستخدام الإنترنت مخططاً بشكل مسبق، ينبغي توجيه الطلاب إلى المواقع الإلكترونية التي تم فحصها مسبقاً للتأكد من أن محتواها مناسب لإستخدامها.
- القيام بحظر معظم المواقع الإلكترونية بإستخدام تصفية الشبكة. وبالتالي ينبغي على المعلمين القيام بتقديم طلب حتى يتم السماح للطلاب بالوصول إلى المواقع. ويتم القيام بفحص جميع المواقع قبل القيام بمنح الإذن وذلك للتأكد من خلوها من أي محتوى غير لائق.
- إعطاء الحرية للطلاب للقيام بعمليات البحث عبر شبكة الإنترنت بإستخدام محركات البحث، إلا أنه ينبغي على المعلمين القيام بمراقبة محتوى المواقع الإلكترونية التي يتم الوصول إليها من قبل الطلاب.
- ضرورة القيام بتوعية الطلاب بمخاطر الإنترنت بجميع الحصص الدراسية ليكونوا على دراية تامة بمحتوى المواقع الإلكترونية الذي يصلون إليه مع توجيههم للتحقق من دقة البيانات.
- ضرورة القيام بتعليم الطلاب حول كيفية التعرف على مصادر المعلومات المستخدمة وإحترام حقوق النشر عند إستخدام البيانات التي يتم الوصول إليها عبر الإنترنت.

سياسة كلمة المرور

سياسة كلمة المرور للإداريين والمعلمين والطلاب

- القيام بإصدار كلمة المرور لجميع المستخدمين عند إنشاء البريد الإلكتروني ومشاركته في البداية.
- البريد الإلكتروني الذي تم إنشاؤه حالياً للإداريين والمعلمين ولجميع الطلاب من مرحلة رياض الأطفال حتى الصف الثاني عشر.
- القيام بمطالبة المستخدمين بتغيير كلمة المرور الخاصة بهم على الفور بمجرد إنشاء الحساب.
- قيام النظام بإقتراح القوة الموصي بها والمعايير المعتمدة لإنشاء كلمات المرور. ولا يتم قبول كلمات المرور التي لاتستوفي المعايير المطلوبة.
- في حالة نسيان كلمة المرور أو الحاجة إلى إعادة تعيين كلمة المرور حال إختراقها، يقوم ولي الأمر بإرسال طلب لإعادة تعيين كلمة المرور إلى المدرسة عبر قنوات التواصل المعتمدة ومن ثم يتم إرسال كلمة المرور الجديدة إلى ولي الأمر الذي تقدم بطلب إعادة التعيين.
- بإمكان الإداريين والمعلمين القيام بطلب المعلومات من فريق الدعم الفني مباشرةً وذلك بالتواصل معهم عبر رقم الهاتف الخاص بالدعم الفني.
- القيام بتحديث كلمات المرور مرتين في العام الدراسي لجميع الطلاب بدءاً من الصف الثالث الإبتدائي حتى الصف الثاني عشر. ويتم تحديث كلمات المرور للإداريين والمعلمين كل 90 يوم.
- القيام بتعيين كلمات المرور لجميع الطلاب بدءاً من مرحلة رياض الأطفال حتى الصف الثاني الإبتدائي مرةً واحدة في العام الدراسي ويقوم مُربيي الصفوف بإرسال كلمات المرور إلى أمور هؤلاء الطلاب من عبر قناة الإتصال معتمدة للمدرسة.

- لا تتوفر قاعدة بيانات لكلمات المرور سواء للإداريين والمعلمين أو الطلاب، حيث أن مسؤول الدعم الفني هو فقط من لديه خيار إعادة التعيين.

وصول الزوار إلى أنظمة تكنولوجيا المعلومات والإتصالات

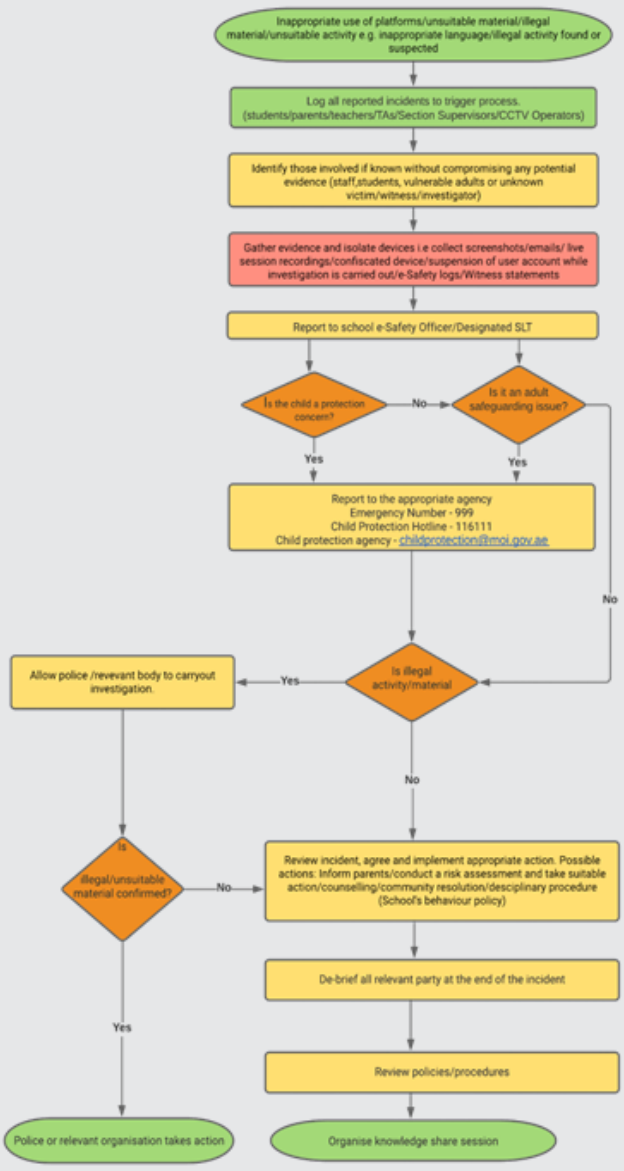
- عدم القيام بمنح الزوار حق الوصول إلى أنظمة تكونولوجيا المعلومات والإتصالات الخاصة بالمدرسة (مثل الملفات والمجلدات).
- يتم منح الزوار فقط كلمة مرور مؤقتة للـ WiFiمن أجل السماح لهم بالوصول إلى شبكة الإنترنت.
- جميع مجموعات المستخدمين (الطلاب والإداريين والمعلمين والزوار) لديهم أسم مستخدم منفصل.

العقوبات:

سيضمن مدير المدرسة بالتنسيق مع مسؤول الأمن الإلكتروني التعامل الصحيح مع أية تهديدات أو جرائم إلكترونية وفقاً لما هو منصوص عليه في لائحة السلوك الطلابي المعتمدة من قبل المدرسة مع القيام بإتخاذ الإجراءات المناسبة حيال ذلك.

- تشمل العقوبات التي يتم تطبيقها حسب الإقتضاء على تعليق وصول الفرد إلى شبكة الإنترنت و/ أو تعليق حساب المستخدم الفردي مؤقتاً.
- بالنسبة للمخالفات الخطيرة (إستمرار الشخص المتنمر في ممارسة التنمر الإلكتروني)، يقرر مدير المدرسة القيام بفصل المسؤول أو المسؤولين عن إرتكاب هذه الجريمة.
- التوصل المنتظم بين مسؤول الأمن الإلكتروني والأخصائيين الإجتماعيين والمعلمين يضمن سرعة التعرف على الطلاب الذين يقعون ضحية للتنمر الإلكتروني سواء على نحو متفرق أو مستمر.
- قيام الأخصائي الإجتماعي عند الضرورة بمطالبة الأشخاص المعنيين بتقديم جميع التقارير والوثائق والمستندات ومن ثم قيام الأخصائي الإجتماعي بالتواصل مع أولياء أمور الطلاب المعنيين.
- في حال وقوع جريمة التنمر الإلكتروني أو غيرها من الجرائم الإلكترونية المدرجة في السياسة المعتمدة من قبل إدارة المدرسة والتي قد تحدث خارج المدرسة، إلا أنها مترابطة بعضوية المدرسة، يقوم مدير المدرسة بفرض عقوبات تأديبية على السلوكيات الغير لائقة.
- قيام إدارة المدرسة بإتباع آليات التعامل الصحيحة مع مثل هذه الحوادث والسلوكيات المرتبطة بها بما في ذلك التنمر الإلكتروني وفقاً لما هو منصوص عليه في سياسة السلامة الإلكترونية، حيث يتم إبلاغ أولياء الأمور بحوادث السلوك المخالفة لقواعد السلامة الإلكترونية والتي تحدث خارج المدرسة.
- في حال عدم الإلتزام بالسياسة، يتم إتخاذ الإجراءات المناسبة وفقاً لما هو منصوص عليه في كلاً ن لائحة الثواب والعقاب ولائحة السلوك الطلابي وسياسة حماية الطفل المعتمدة من قبل المدرسة.

إجراءات تسجيل حوادث السلامة الإلكترونية:



ليـــوا للتعليم
Liwa Education

ملكية السياسات

إدارة التعليم التقني

الأطراف المعنية الرئيسة		
مالك السياسة	ساندرا تيشاجوا	مدير التعليم التقني – ليوا للتعليم
تمت مراجعتها من قبل:		
	السيد. كيفن والاس	نائب مدير عام ليوا للتعليم
تمت الموافقة عليها من قبل:	د. شيرين جبران	مدير عام ليوا للتعليم