اكاديمية الدوحة
DOHA ACADEMY

سياسة السلامة الإلكترونية 2025/2024

1. الغرض:

تهدف سياسة السلامة الإلكترونية في أكاديمية الدوحة إلى إرساء إطار عمل شامل لحماية طلابنا أثناء استخدامهم للتقنيات الرقمية داخل مجتمعنا المدرسي. تُحدد هذه السياسة التزامنا بتهيئة بيئة إلكترونية آمنة، ووضع معايير عالية للسلوك الإلكتروني، وضمان الاستخدام المسؤول للإنترنت والأجهزة الرقمية دعمًا للتعليم والتعلم.

2. النطاق:

تُطبق هذه السياسة على جميع الطلاب والموظفين وأعضاء مجتمعنا المدرسي الذين يستخدمون التقنيات الرقمية ويتصلون بالإنترنت داخل المدرسة أو أثناء الأنشطة المدرسية.

3. بيان السياسة:

تلتزم مدرستنا بضمان سلامة ورفاهية طلابنا في العصر الرقمي. ندرك أهمية تسخير التكنولوجيا لأغراض تعليمية، مع حماية الطلاب من مخاطر الإنترنت المحتملة.

4. التعليم والتعلم:

4.1 يهدف استخدام الطلاب للإنترنت في أكاديمية الدوحة إلى تعزيز تعلمهم. ولتحقيق هذه الغاية، سيتم تثقيف الطلاب حول الاستخدام الفعال للإنترنت في البحث، بما في ذلك مهارات تحديد مصادر المعرفة واسترجاعها وتقييمها.

4.2 سيتم تدريب الطلاب على الوعي النقدي بالمواد الإلكترونية التي يقرؤونها، وكيفية التحقق من صحة المعلومات قبل قبولها. ستضمن المدرسة أن استخدام الطلاب للمواد التي يحصلون عليها يتوافق مع الأمانة الأكاديمية.

4.3 سيتم تعليم الطلاب ما هو مقبول وما هو غير مقبول لاستخدام الإنترنت، وتزويدهم بأهداف واضحة لاستخدامه. سيتم إعلام الطلاب بمراقبة استخدام الشبكة والإنترنت، ومتابعة الاستخدام غير المناسب بشكل مناسب.

4.3 من خلال التجمعات، وعلوم الحاسوب، وتكنولوجيا المعلومات، والتربية الشخصية والاجتماعية والصحية، يتعلم الطلاب كيفية التصرف وحماية أنفسهم في البيئة الرقمية. مع ذلك، لا تتحمل المدرسة مسؤولية أي أحداث تقع خارج المدرسة.

4.5 سيتم فحص التقنيات الناشئة للتحقق من فائدتها التعليمية قبل السماح باستخدامها في المدرسة.

4.6 يُطلب من الموظفين مراجعة المواد التي يتم الحصول عليها من الإنترنت بعناية وتكييفها لدعم العمل المدرسي لضمان توافقها مع القيم الإسلامية.

5 التنمر الإلكتروني:

5.1 تأخذ أكاديمية الدوحة قضية التنمر الإلكتروني ووقوعه على محمل الجد. يُقدّم محتوى تعليمي حول التنمر الإلكتروني للطلاب، بالإضافة إلى دروس تكنولوجيا المعلومات والاتصالات

5.2 تلتزم المدرسة بتثقيف الطلاب حول عواقب التنمر الإلكتروني وأهمية التفاعلات المحترمة عبر الإنترنت.

5.3 في حال علم المدرسة بأي حادثة تنمر إلكتروني داخلها، فإن الإجراءات والعواقب هي نفسها المُطبقة على حالات التنمر غير الإلكتروني، كما هو مُحدد في إدارة السلوك ومكافحة التنمر في أكاديمية الدوحة والسياسات والإجراءات ذات الصلة.

6 الوصول إلى الإنترنت / الأمن السيبراني:

6.1 صُممت خدمة الإنترنت في أكاديمية الدوحة خصيصًا لاستخدام الطلاب، وتتضمن فلترة مناسبة لأعمارهم. وتضمن المدرسة مراجعة الفلترة وتحسينها بانتظام. كما يتم تحديث برامج الحماية من الفيروسات بانتظام، كما يتم تحديث هذا الجانب من أمن الإنترنت بشكل منهجي.

6.2 إذا اكتشف الموظفون أو الطلاب، حتى داخل البيئة الرقمية المُفلترة، موقعًا غير مناسب، فيجب إبلاغ فريق دعم تكنولوجيا المعلومات لاتخاذ الإجراءات اللازمة.

6.3 ستتخذ المدرسة جميع الاحتياطات المعقولة لمنع الوصول إلى المواد غير المناسبة. ومع ذلك، نظرًا للنطاق الدولي وطبيعة محتوى الإنترنت المترابطة، لا يمكن ضمان عدم ظهور المواد غير المناسبة على جهاز كمبيوتر المدرسة. ولا تتحمل المدرسة مسؤولية المواد التي يتم الوصول إليها، أو أي عواقب تترتب على الوصول إلى الإنترنت.

6.4 شبكات التواصل الاجتماعي والنشر الشخصي: ستمنع المدرسة الوصول إلى مواقع التواصل الاجتماعي، ويُنصح الطلاب بعدم استخدامها في المنزل حتى يبلغوا السن التي يحددها مسؤولو الموقع.

6.5 الأجهزة الشخصية: يُحدد استخدام الطلاب للأجهزة الشخصية في إرشادات أكاديمية الدوحة الخاصة بإحضار أجهزتهم الخاصة . يُسمح باستخدام الهواتف المحمولة فقط في الدروس التي تُجرى تحت إشراف المعلم. يجب معاملة الأجهزة القابلة للارتداء، مثل الساعات الذكية، بنفس طريقة معاملة الأجهزة الأخرى التي تتيح الاتصال بالإنترنت.

6.6 أثناء اتصال الطلاب بشبكة المدرسة، يخضعون لقيود أمنية وتصفية. يُطلب من الطلاب تسليم أي هاتف ذكي أحضروه إلى المدرسة، وألا يحتوي أي جهاز آخر ضمن مبادرة إحضار الأجهزة الشخصية على شريحة SIM خاصية الوصول إلى الإنترنت الخارجي. في حال استخدام شبكة جوال، بما يخالف إرشادات المدرسة، فإن المدرسة غير مسؤولة عما يصل إليه الطلاب.

6.7 إذا أحضر طالب هاتفًا محمولًا إلى المدرسة، وثبت استخدامه لالتقاط الصور أو مقاطع الفيديو داخل المدرسة، أو وجود صور غير لائقة أو مخبأة عليه، أو وجود دليل على التنمر الإلكتروني، فسيتم التعامل مع ذلك كمسألة تأديبية خطيرة، وسيتم اتخاذ إجراءات إضافية.

7 مخاوف وشكاوى السلامة الإلكترونية:

7.1 سيتعامل أعضاء فريق القيادة العليا بالمدرسة مع مخاوف أولياء الأمور أو الطلاب بشأن السلامة الإلكترونية وفقًا لإجراءات الشكاوى المتبعة في المدرسة، مع تصعيد الأمور إلى مستوى مدير المدرسة حسب الاقتضاء.

7.2 يجب إحالة أي شكوى تتعلق بإساءة استخدام الموظفين للإنترنت إلى رئيس المدرسة/مدير المدرسة.

7.3 يجب التعامل مع الشكاوى المتعلقة بحماية الطفل فورًا وفقًا لسياسة حماية الطفل في أكاديمية الدوحة والإجراءات ذات الصلة.

8 الأدوار والمسؤوليات:

على مدير المدرسة:	أن يكون جهة الاتصال في حال حدوث أي سوء سلوك من قبل الموظفين فيما يتعلق باستخدام الإنترنت.
على رؤساء المدارس:	متابعة حالات سوء سلوك الطلاب فيما يتعلق باستخدام الإنترنت.
على المعلمين:	• تقديم محتوى حول السلامة الإلكترونية وتذكير الطلاب عند استخدام الأجهزة المحمولة في مجالات دراسية أخرى؛ • تطبيق هذه السياسة؛ • التعامل مع قضايا التنمر الإلكتروني، وتسجيل مثل هذه الحوادث على نظام معلومات إدارة المدرسة (ISAMS)؛ • معاينة أي محتوى على الإنترنت يعتزمون مشاركته مع الطلاب.
على مسؤولي السلامة المعينين:	مسؤولي الحماية المعينين: • اتباع سياسات حماية الطفل والحماية والتصفية ذات الصلة • ومراقبة حالات إساءة معاملة الأطفال عبر الإنترنت.
على الطلاب:	اتباع إرشادات المدرسة ولوائحها المتعلقة باستخدام الأجهزة الشخصية والإنترنت.
على أولياء الأمور:	دعم سياسة وإرشادات السلامة الإلكترونية في المدرسة.
على مسؤول شبكة تكنولوجيا المعلومات:	• تحمل المسؤولية الشاملة عن السلامة الإلكترونية في المدرسة؛ • إزالة إمكانية الوصول إلى المواقع غير المناسبة بناءً على طلب هيئة التدريس؛ • تحمل مسؤولية أمن نظام المدرسة (بما في ذلك الفلترة والحماية من الفيروسات) تحت إشراف رئيس دعم تكنولوجيا المعلومات.

9 الوثائق ذات الصلة:

- سياسات الاستخدام المقبول للموظفين والطلاب
- سياسة إحضار جهازك الخاص
- سياسات إدارة السلوك
- سياسة مكافحة التنمر
- سياسة حماية الطفل وسلامته
- إجراءات التصفية والمراقبة

اسم السياسة: السلامة الإلكترونية 2025/2024		
تاريخ الإنشاء: أغسطس 2023	**تاريخ آخر مراجعة:** مارس 2025	**تاريخ المراجعة التالية:** أغسطس 2025
مُعتمد من المدير: **التوقيع:**		**مُعتمد من الرئيس التنفيذي:** **التوقيع:**
ختم المدرسة:		**ختم المجموعة:**