



سياسة المدرسة في الأمن السيبراني

للعام 2026-2027

المقدمة

تلتزم المدرسة بتوفير بيئة تعليمية آمنة ورقمية سليمة، خالية من كافة التهديدات السيبرانية التي قد تُعرض خصوصية الطلبة للخطر أو تُعيق نموهم الأكاديمي والنفسي. وانطلاقاً من مسؤوليتها التربوية، تُولي المدرسة اهتماماً بالغاً بحماية البنية التحتية الرقمية، وضمان الاستخدام الآمن والمسؤول للتقنيات الحديثة من قبل جميع أفراد المجتمع المدرسي. وتُعد هذه السياسة امتداداً لجهود المدرسة المستمرة في تعزيز الوعي الأمني السيبراني، وترسيخ ثقافة الحماية الرقمية، وتعزيز قيم المسؤولية الشخصية والانضباط الذاتي في التعامل مع الوسائط الإلكترونية داخل البيئة التعليمية.

أهداف السياسة

1. الحد من المخاطر السيبرانية داخل البيئة المدرسية، بما يضمن بيئة تعليمية رقمية آمنة وخالية من التهديدات الإلكترونية التي قد تُعرض خصوصية الطلبة وسلامة المعلومات للخطر.
2. رفع مستوى الوعي لدى الطلبة والكادرين التعليمي والإداري حول أهمية الأمن السيبراني، والممارسات السليمة في استخدام التقنية، والآثار السلبية الناجمة عن السلوكيات الرقمية غير الآمنة.
3. تعزيز بيئة مدرسية رقمية محفزة وآمنة، تشجع على الاستخدام المسؤول للتكنولوجيا، وتدعم قيم الانضباط الذاتي والاحترام المتبادل في الفضاء الإلكتروني.
4. تفعيل آليات الكشف المبكر عن السلوكيات الرقمية الخطرة أو غير الأخلاقية، مثل التمر الإلكتروني أو اختراق الأنظمة، وتقديم الدعم التربوي والتقني المناسب للحالات المتأثرة.
5. تطبيق الإجراءات التأديبية والتربوية وفقاً للأنظمة المعتمدة بحق من يثبت تورطه في انتهاك قواعد الأمن السيبراني، بما يحقق الردع ويعزز العدالة الرقمية داخل المجتمع المدرسي.
6. تعزيز التعاون والتنسيق مع الجهات المختصة في مجال الأمن السيبراني لضمان استمرارية الحماية الرقمية، ودعم جهود التوعية والوقاية على مستوى المدرسة والمجتمع.
7. توفير أعلى درجات الحماية لشبكة المدرسة بأحدث نسخة للحماية Firewall لضمان حماية البيانات ومنع القرصنة والاختراق.



المبادئ الأساسية

- الوقاية أولاً: تُعد التوعية والتثقيف الرقمي حجر الأساس في الحد من السلوكيات الإلكترونية الضارة، وتعزيز الاستخدام الآمن والمسؤول للتكنولوجيا.
- السرية: تُراعى السرية التامة في التعامل مع أي خرق أو حادث سيبراني، حفاظاً على خصوصية الطلبة وكافة أفراد المجتمع المدرسي.
- المصلحة الفضلى للطلاب: تُؤخذ بعين الاعتبار في جميع التدخلات والإجراءات المتعلقة بالأمن السيبراني، بما يضمن حماية الطالب ودعمه تربوياً وتقنياً.
- المساواة: يخضع كل من يثبت تورطه في انتهاك قواعد الأمن السيبراني للمساءلة وفقاً للوائح المدرسية والقوانين المعمول بها، بما يحقق العدالة الرقمية ويعزز الانضباط.

الوقاية والتوعية

1. ضمان حصول المدرسة على أحدث نسخة لجدار الحماية لشبكة المدرسة Firewall.
2. تنفيذ حملات توعوية دورية داخل المدرسة، تتضمن ملصقات إرشادية، عروض تقديمية، ومبادرات طلابية تهدف إلى نشر ثقافة الاستخدام الآمن والمسؤول للتكنولوجيا.
3. إدماج مفاهيم الأمن السيبراني ضمن الأنشطة الصفية واللاصفية، بما يعزز الفهم العميق لدى الطلبة حول التهديدات الرقمية، مثل التنمر الإلكتروني، اختراق الخصوصية، والاحتيال الإلكتروني.
4. تنظيم ورش عمل ومحاضرات تثقيفية بالتعاون مع الجهات المختصة في الأمن السيبراني، لتقديم معلومات دقيقة ومؤثرة بأسلوب يناسب الفئة العمرية المستهدفة، ويعزز مهارات الحماية الرقمية.
5. تدريب الكادر التعليمي والإداري على رصد السلوكيات الرقمية غير الآمنة، وتزويدهم بآليات التدخل الأولي والتعامل التربوي السليم مع الحوادث السيبرانية.
6. إشراك أولياء الأمور في برامج التوعية الرقمية من خلال نشرات تثقيفية ولقاءات دورية، لتعزيز دور الأسرة في التوجيه والمتابعة، وضمان الاستخدام الآمن للتقنيات في المنزل.
7. تفعيل دور الأخصائيين الاجتماعيين والنفسيين في تقديم جلسات إرشادية فردية وجماعية، لمعالجة الآثار النفسية الناتجة عن الحوادث السيبرانية، وتوفير بيئة آمنة للطلبة للتعبير عن مخاوفهم الرقمية.
8. إطلاق مبادرات طلابية قيادية مثل "سفراء الأمن الرقمي" لتمكين الطلبة من نشر الوعي بين أقرانهم، وتعزيز ثقافة المسؤولية الجماعية في الفضاء الإلكتروني.



الرصد والكشف المبكر

تؤدي المدرسة أهمية بالغة لعمليات الرصد والكشف المبكر، باعتبارها خطوة جوهرية في الوقاية من السلوكيات الرقمية الضارة، وضمان بيئة تعليمية آمنة ومحصنة إلكترونياً. ويتم ذلك من خلال:

- مراقبة جميع المواقع التي يتصفحها الطلبة، وحظر جميع المواقع التي يمكن أن تهدد سلامة الطلبة الإلكترونية عن طريق Server.
- المتابعة المستمرة لسلوك الطلبة في البيئة الرقمية المدرسية، مع التركيز على رصد أي تغيرات في نمط الاستخدام أو التفاعل الإلكتروني قد تشير إلى وجود خطر محتمل، مثل التتمر الإلكتروني، محاولات الاختراق، أو تداول محتوى غير لائق.
- استقبال البلاغات بسرية تامة من قبل منسق الحماية أو الأخصائي الاجتماعي والنفسي، مع ضمان حماية خصوصية الطالب وعدم تعريضه لأي وصم أو تمييز رقمي أو اجتماعي.
- إجراء لقاءات فردية مع الطلبة الذين تظهر عليهم مؤشرات أو سلوكيات رقمية مثيرة للقلق، مثل الاستخدام المفرط أو غير الآمن للمنصات الإلكترونية، وتشمل هذه اللقاءات:
 - ❖ الحفاظ على السرية التامة من قبل الأخصائي الاجتماعي أو النفسي، وبمشاركة منسق الحماية في المدرسة.
 - ❖ استخدام أدوات تقييم تربوية ونفسية مثل الاستبانات الرقمية أو تحليل السلوك الإلكتروني.
 - ❖ الاستماع للطالب باحترام وحيادية لفهم دوافعه وسلوكياته الرقمية وظروفه الشخصية.
 - ❖ تحليل البيئة المحيطة بالطالب (الأسرة، الأصدقاء، المحتوى الرقمي، المدرسة) لتحديد مصادر التأثير السيبراني.
 - ❖ تحديد نوع التدخل المناسب بناءً على نتائج التقييم، مثل جلسات إرشادية، إشراك ولي الأمر، أو تحويل الحالة للجهات المختصة في الأمن السيبراني أو الدعم النفسي.

الإلتزامات والإبلاغ

يتوجب على جميع العاملين في المدرسة من أعضاء الهيئة التدريسية والإدارية والفنية و فرق الخدمات المساندة (بما في ذلك المعلمون، الإداريون، الأخصائيون الاجتماعيون والنفسيون، موظفو الأمن، وعمال المدرسة)، الإلتزام برصد أي مؤشرات رقمية أو سلوكية قد تُشير إلى وجود خطر محتمل يهدد سلامة الطالب في البيئة الإلكترونية. ويشمل ذلك التدخل الأولي والتعامل التربوي السليم، مع ضرورة الإبلاغ الفوري عن أي حالة مشتبه بها أو مؤكدة تتعلق بسلوكيات رقمية ضارة مثل التتمر الإلكتروني، اختراق الخصوصية، أو تداول محتوى غير لائق، وذلك وفقاً للإجراءات المعتمدة في السياسة المدرسية للأمن السيبراني.



أعضاء سياسة الأمن السيبراني

الأدوار والمسؤوليات في سياسة الأمن السيبراني:

➤ إدارة المدرسة

1. تلتزم الإدارة المدرسية بتطبيق سياسة الأمن السيبراني بما يتوافق مع التشريعات الوطنية والمعايير التربوية، لضمان بيئة تعليمية رقمية آمنة ومحفزة.
2. تنظيم برامج تدريبية دورية لجميع العاملين حول التهديدات السيبرانية، وآليات الرصد والتبليغ والتدخل.
3. رفع مستوى الوعي لدى الطلبة وأولياء الأمور حول مخاطر السلوكيات الرقمية غير الآمنة، ووسائل الوقاية والدعم.
4. متابعة تنفيذ السياسة وتقييم فعاليتها بشكل دوري، وتحديث الإجراءات وفقاً للمستجدات التقنية والقانونية.
5. ضمان وجود آلية سرية لتلقي البلاغات السيبرانية، والإشراف على توثيقها والتنسيق مع الجهات المختصة حسب الإجراءات المعتمدة.

➤ منسق حماية الطفل (Child Protection Officer)

1. استقبال البلاغات المتعلقة بالانتهاكات السيبرانية والتعامل معها بسرية تامة.
2. التنسيق مع الجهات المختصة (مثل شرطة دبي وهيئة تنظيم الاتصالات) عند الحاجة.
3. متابعة تطبيق السياسات والإجراءات الوقائية داخل المدرسة.
4. إعداد تقارير دورية لإدارة المدرسة حول الحالات المكتشفة والتدخلات المنفذة.

➤ الكادر الإداري والمعلمون

1. متابعة سلوك الطلبة في البيئة الرقمية، ورصد أي مؤشرات قد تدل على تعرضهم لمخاطر مثل التنمر الإلكتروني أو اختراق الخصوصية.
2. الالتزام بالإبلاغ الفوري عن أي حالة مشتبه بها أو مؤكدة وفقاً للسياسة المعتمدة.
3. تعزيز بيئة مدرسية رقمية قائمة على الاحترام والثقة، وتشجيع الطلبة على طلب المساعدة عند الحاجة.



➤ أولياء الأمور

- التعاون المستمر مع المدرسة لضمان سلامة الأبناء الرقمية وحمايتهم من السلوكيات الإلكترونية الضارة.
- الإبلاغ الفوري عن أي خطر أو سلوك مشبوه يتعلق بالطالب داخل أو خارج البيئة الرقمية.
- المشاركة في الأنشطة التوعوية والبرامج الإرشادية التي تنظمها المدرسة في مجال الأمن السيبراني.

➤ الطلاب

- الالتزام بالسلوكيات الرقمية الإيجابية داخل المدرسة وخارجها.
- معرفة حقوقهم وآليات طلب الدعم والمساعدة في حال التعرض لأي تهديد إلكتروني.
- المساهمة في نشر ثقافة الحماية الرقمية بين الأقران من خلال المبادرات الطلابية.
- الالتزام بالإجراءات المتبعة بحق من يثبت تورطه في انتهاك قواعد الأمن السيبراني.

➤ الأخصائيون الاجتماعيون والنفسيون

الدور الوقائي:

1. نشر الوعي بين الطلبة وأولياء الأمور حول مخاطر السلوكيات الرقمية غير الآمنة، وأهمية الوقاية المبكرة.
2. تنفيذ برامج إرشادية وتوعوية منتظمة حول المهارات الرقمية، وضبط النفس، واتخاذ القرار في الفضاء الإلكتروني.
3. تعزيز بيئة مدرسية داعمة تشجع على التسامح والاحترام، وتنبذ كافة أشكال السلوكيات السيبرانية الضارة.
4. المساهمة في تطوير السياسات والخطط الوقائية بالتعاون مع إدارة المدرسة.

الرصد والكشف المبكر:

1. مراقبة التغيرات النفسية والسلوكية لدى الطلبة التي قد تشير إلى تعرضهم لمخاطر رقمية.
2. إجراء مقابلات تقييمية فردية عند الاشتباه، بالتعاون مع الفريق الإرشادي.
3. التنسيق مع الكادر التعليمي لتحديد الطلبة المعرضين للخطر، وضمان توثيق الحالات وفقاً للسياسة المتبعة.



التدخل والتبليغ:

1. استقبال البلاغات بسرية تامة والتعامل معها وفقاً لبروتوكول التحويل الداخلي المعتمد.
2. إجراء تقييم أولي للحالة بالتعاون مع الجهات المعنية داخل المدرسة.
3. التواصل مع الجهات الخارجية المختصة عند الحاجة، مثل هيئة تنظيم الاتصالات وشرطة دبي.
4. إعداد خطة تدخل فردية لدعم الطالب المتضرر، تشمل الجوانب النفسية والتربوية.

الدعم والمتابعة:

1. تقديم الدعم النفسي الفردي أو الجماعي للطلبة المتأثرين بالحوادث السيبرانية.
2. متابعة الحالات بعد التدخل لضمان استقرار الطالب وسلامته النفسية والجسدية.
3. التنسيق مع الأسرة لتوفير بيئة رقمية داعمة داخل وخارج المدرسة.
4. توثيق جميع الإجراءات والتدخلات بدقة وسرية تامة، وفقاً للسياسة المعتمدة.

إجراءات التبليغ والتعامل مع الحالات

➤ الأدوار والمسؤوليات في سياسة الأمن السيبراني

1. **منسق حماية الطفل (Child Protection Officer):** يتولى استقبال البلاغات المتعلقة بالانتهاكات السيبرانية التي تمس سلامة الطلبة الرقمية، ويقوم بالتعامل معها بسرية تامة، مع التنسيق مع الجهات المختصة مثل شرطة دبي وهيئة تنظيم الاتصالات عند الحاجة، وفقاً للبروتوكولات المعتمدة.
2. **المعلمون والإداريون:** يُعدّون خط الدفاع الأول في رصد السلوكيات الرقمية غير الآمنة، ويلتزمون قانونياً بالإبلاغ الفوري عن أي اشتباه في حالات التنمر الإلكتروني، اختراق الخصوصية، أو تداول محتوى ضار، وذلك من خلال رفع البلاغ إلى منسق حماية الطفل أو إدارة المدرسة دون تأخير.
3. **المرشدون الاجتماعيون والنفسيون:** يؤدون دوراً محورياً في تقديم الدعم النفسي والاجتماعي للطلبة المتأثرين بالحوادث السيبرانية، ويشاركون في تقييم الحالات الرقمية المثيرة للقلق، وتحليل دوافعها، وتقديم التوصيات المناسبة وفقاً للإجراءات المعتمدة، بما يضمن التدخل السليم والدعم المستمر.



خطوات التبليغ داخل المدرسة في حالات الانتهاك السيبراني

1. رصد المؤشرات يتعين على الكادر التعليمي والإداري، بالإضافة إلى المرشدين الاجتماعيين والنفسيين، متابعة سلوك الطلبة في البيئة الرقمية والانتباه لأي علامات قد تدل على تعرضهم لمخاطر سيبرانية مثل التنمر الإلكتروني، اختراق الخصوصية، أو تداول محتوى ضار.
2. الإبلاغ الداخلي عند الاشتباه، يجب التبليغ الفوري لمنسق حماية الطفل أو إدارة المدرسة وفقاً للآلية المعتمدة، لضمان التدخل السريع والفعال.
3. توثيق الحالة يتم تسجيل كافة التفاصيل المتعلقة بالحالة بسرية تامة، مع الحفاظ الكامل على خصوصية الطالب، وفقاً للسياسات المعتمدة لحماية البيانات.
4. التواصل الخارجي في الحالات التي تستدعي تدخلاً رسمياً، مثل الانتهاكات الجسيمة أو التهديد المباشر لسلامة الطالب أو زملائه، يتم التواصل مع الجهات المختصة لضمان الحماية واتخاذ الإجراءات اللازمة.

قنوات التبليغ الرسمية خارج المدرسة

تلتزم المدرسة بإبلاغ الجهات المختصة خارج نطاقها في حال رصد حالات اختراق أو استغلال إلكتروني جسيم، أو في حال استمرار السلوك الضار رغم التدخل المدرسي، أو عند وجود خطر مباشر يهدد سلامة الطالب أو زملائه. ويتم التواصل مع الجهات الرسمية المعنية وفقاً للتشريعات الوطنية المعمول بها، عبر القنوات التالية:

- وزارة الداخلية – الخط الساخن لحماية الطفل 116111 :
- هيئة تنظيم الاتصالات – مركز الاستجابة لطوارئ الحاسب الآلي (aeCERT)
- شرطة دبي – قسم الجرائم الإلكترونية 901 :
- مؤسسة دبي لرعاية النساء والأطفال 800111 :

التقييم

تُراجع هذه السياسة سنوياً من قبل لجنة مختصة، ويتم تحديثها بناءً على المستجدات القانونية والتقنية، مع إشراك المعنيين من الكادر التعليمي والطلبة وأولياء الأمور لضمان فعاليتها واستمراريتها، ومواكبتها لأحدث التحديات السيبرانية



Al Rashid Al Saleh Private School

مدرسة الراشد الصالح الخاصة

أخر تحديث: 2025/9/22 مدرسة متميزة ، تخرج أجيالاً تعتز بأصالتها ، وتحافظ على هويتها ، وتشارك في بناء مستقبل وطنها.

QM-114

آخر تحديث 2025/9/22