سياسة الأمن الرقمي داخل المدرسة

تشمل **الحماية من أخطار الشبكة العالمية للمعلومات** التدابير المتخذة التالية:

1. وقاية الطلبة من التعرض لمواد واتصالات وسلوكيات ضارة على الإنترنت، من خلال استخدام SONICWALL وهو نظام موثوق به لتنقية مواقع الشبكة العالمية للمعلومات، وتنبيه مدير المدرسة والمعلمين عند استخدام الطلبة المواد غير اللائقة على الإنترنت، ومنع الطلبة من الوصول إلى المواقع المنافية للأخلاق وغيرها من المواقع غير المناسبة.
2. منع الأشخاص غير المرخص لهم من الوصول إلى بيانات المدرسة.
3. تعريف الطلبة بمخاطر **التنمر الإلكتروني** بمنعهم من استخدام الأجهزة الإلكترونية والمعلوماتية مثل البريد الإلكتروني والرسائل الفورية والرسائل النصية والهواتف المحمولة ومواقع الإنترنت لإرسال الرسائل أو نشر- الصور التي من شأنها أن تلحق ضررًا بشخص أو مجموعة ما.
4. تثقيف الطلبة حول الاستخدام السليم للإنترنت وتبادل المعلومات الشخصية.
5. توعية الطالب ليكون قادرًا على معرفة أشكال مختلفة من التنمر الإلكتروني، ومعرفة الخطوات التي يجب اتخاذها في حال واجه مثل هذا السلوك.
6. نشر الممارسات الجيدة في مجال الاستخدام الآمن لأنظمة الإنترنت.
7. منع مشاهدة أي مواد غير لائقة أو تحميلها(الملحوظات أو التعليقات المنافية للأخلاق، والتهكم، أو أي نوع من أنواع التعليقات الأخرى التي يمكن أن تسيء لشخص ما على أساس الإعاقة الجسدية أو العقلية أو السن أو الدين أو الحالة الاجتماعية أو الانتماءات السياسية أو العرق.)
8. مراقبة استخدام الإنترنت من قسم تكنولوجيا المعلومات في المدرسة.
9. قيام المعلمين وأمناء المكتبات بدور فعال في حماية الطلبة من مخاطر الإنترنت، ومراقبة المواقع الإلكترونية التي يدخلها الطلبة، التحقق من الهدف الأكاديمي للطلبة قبل السماح لهم باستخدام الإنترنت(لا ينبغي أن يسمح للطلبة بالإبحار عبثًا دون هدف معين على شبكة الإنترنت.) ومراقبتهم في أثناء الرحلات المدرسية في حال استخدامهم أيًّا من الأجهزة الإلكترونية المتصلة بشبكة الإنترنت.
10. توجيه الطلبة خلال النشاطات الإلكترونية التي من شأنها أن تدعم مخرجات التعلم المخطط لها وفقا لسن الطالب ودرجة نضجه.
11. يمنع استخدام الإنترنت لمحاولة الوصول غير المصرح به إلى أجهزة الكمبيوتر الأخرى والمعلومات أو الخدمات المحظورة.
12. عدم فتح البريد الإلكتروني أو المرفقات من مصادر غير معروفة.
13. منع تحميل المواد محفوظة الحقوق أو نسخها، بما في ذلك البرمجيات والكتب والمقالات والصور وما إلى ذلك إن لم تملك المدرسة رخصة لاستخدامها.
14. منع القيام بأي نشاط يمكن أن يتسبب في نقل فيروسات أو برامج ضارة أخرى إلى شبكة المدرسة.
15. التأكد من أن المعلومات الشخصية المتاحة في المدرسة عن طريق الإنترنت والإنترانت آمنة، حتى فيما يتعلق بالمواقع الإلكترونية المحمية بكلمة مرور.
16. وضع جدول زمني للتطوير المهني المستمر؛ لإبقاء المعلمين على بينة من أحدث تطورات السلامة على الإنترنت.
17. مراجعة البنية التحتية لتكنولوجيا المدرسة بشكل دوري مع الموظفين المختصين في التكنولوجيا وإجراء التحسينات اللازمة عليها.

إدارة المدرسة