سياسة السلامة الرقمية – مجمّع زايد التعليمي - الظيت

تم التطبيق في: سبتمبر 2024
آخر تحديث: مارس 2025
تاريخ المراجعة: يونيو 2025

جدول المحتويات

1. ما هي السلامة الإلكترونية؟
تعريف GCS للسلامة الإلكترونية: الاستخدام الآمن والمسؤول للتكنولوجيا، بما يشمل الإنترنت ووسائل الاتصال الأخرى مثل الرسائل النصية، وأجهزة الألعاب، والبريد الإلكتروني وغيرها. تعنى السلامة الإلكترونية بالسلوك بقدر ما تُعنى بالأمن الإلكتروني.

2. نطاق السياسة
تنطبق على جميع أعضاء المدرسة: الموظفون، الطلاب، المتطوعون، أولياء الأمور/مقدمو الرعاية، الزوار، ومستخدمو المجتمع عند استخدام أو الوصول إلى أنظمة المدرسة لتكنولوجيا المعلومات والاتصالات.

يجب قراءة هذه السياسة بالاقتران مع سياسات المدرسة الأخرى: حماية الطفل، السلوك، التعلم عن بُعد، الاستخدام المقبول، الإدماج، مكافحة التنمر، وغيرها.

3. الغرض من التطبيق
- حماية الأطفال من الأذى.
- حماية الموظفين أثناء التعامل مع الطلاب أو استخدام الإنترنت.
- ضمان وفاء المدرسة بواجبها في رعاية الطلاب.
- توفير توقعات واضحة بشأن الاستخدام المقبول للإنترنت.

4. أهمية الإنترنت
- الإنترنت عنصر أساسي للتعليم والتفاعل الاجتماعي.
- المدرسة مسؤولة عن توفير وصول آمن وذي جودة للطلاب.
- الاستخدام جزء من المنهاج الدراسي في المملكة المتحدة والإمارات.
- الطلاب بحاجة لتعلم تقييم المعلومات وحماية أنفسهم.

5. المخاطر
تشمل: المحتوى، التواصل، والسلوك عبر الإنترنت. قد يؤدي ذلك إلى التنمر الإلكتروني، الوصول إلى محتوى غير قانوني، الاستدراج الجنسي، الانتهاكات المتعلقة بالخصوصية، الإفراط في استخدام التكنولوجيا، الابتزاز، وغيرها.

6. القيادة والمسؤوليات
مجلس الأمناء
- اعتماد السياسة ومراجعة فعاليتها.
- تلقي تقارير منتظمة عن الحوادث.
- تعيين حاكملأ للسلامة الإلكترونية.

القادة الكبار
- ضمان رعاية وسلامة المجتمع المدرسي.

- متابعة التدريب للموظفين.
- دعم الموظفين المسؤولين عن المراقبة الداخلية.

منسق السلامة الإلكترونية
- قيادة فريق السلامة الإلكترونية.
- التحقيق في قضايا السلامة الإلكترونية.
- تدريب الموظفين والتعاون مع الطاقم الفني.

مسؤول حماية الطفل
- متابعة قضايا السلامة الإلكترونية وحماية الطفل.
- التعرف على المخاطر المحتملة عبر الإنترنت.

فريق دعم تكنولوجيا المعلومات
- ضمان البنية التحتية آمنة.
- تطبيق سياسات الترشيح والمراقبة.
- متابعة آخر التطورات التقنية.

المعلمون وموظفو الدعم
- الالتزام بالسياسات والإبلاغ عن المخالفات.
- دمج قضايا السلامة الإلكترونية في المناهج.
- مراقبة استخدام التكنولوجيا في الصف.

الطلاب
- استخدام التكنولوجيا وفق سياسة الاستخدام المقبول.
- حماية المعلومات الشخصية والإبلاغ عن المخالفات.

أولياء الأمور
- دعم أبناءهم في الاستخدام المسؤول للتكنولوجيا.
- الالتزام بإرشادات استخدام الصور والفيديو.

مستخدمو المجتمع
- توقيع اتفاقية استخدام مقبول قبل منح حق الوصول.

7. الاستخدام المقبول للتكنولوجيا
- استخدام الأنظمة للأغراض التعليمية والمهنية.
- حماية كلمات المرور والبيانات الشخصية.
- الالتزام بالتصفية ومراقبة المحتوى.

- التدريب والإرشاد المستمر للطلاب والموظفين.

8. الصور والفيديو
- الالتزام بخصوصية الطلاب وعدم مشاركة الصور والفيديو دون إذن.
- استخدام الأجهزة المدرسية فقط للالتقاط.
- مراعاة اللباس والسلوك عند التصوير.

9. حماية البيانات
- الالتزام بقانون حماية البيانات.
- تقليل استخدام البيانات الشخصية لأدنى حد.
- تأمين البيانات وحمايتها من التسرب.
- توفير وصول آمن للموظفين والطلاب.

10. الاتصال والتواصل
- استخدام البريد الإلكتروني الرسمي للمدرسة.
- الإبلاغ عن أي محتوى مسيء أو تهديدي.
- الالتزام بالاحترافية عند التواصل الرقمي.

11. وسائل التواصل الاجتماعي
- استخدام مسؤول للمنصات الرقمية.
- عدم نشر محتوى مسيء أو إلحاق الضرر بالمدرسة أو الأفراد.
- الحفاظ على الخصوصية وتحديث إعدادات الأمان.

12. المراقبة
- مراقبة استخدام الإنترنت والبريد الإلكتروني.
- تطبيق التصفية والمراقبة وفق عمر الطلاب.
- حفظ السجلات بشكل آمن وموثق.

13. إجراءات الحوادث
- الإبلاغ الفوري والتحقيق العادل.
- تطبيق الإجراءات التأديبية عند الحاجة.
- إشراك أولياء الأمور والشرطة عند الضرورة.
- تسجيل الأدلة والاحتفاظ بها.

14. التدريب والتوعية
- برامج تدريبية دورية للموظفين.
- إدماج برامج توعية للطلاب حول الاستخدام الآمن للإنترنت.

- جلسات توجيهية لأولياء الأمور حول السلامة الإلكترونية.

15. مراجعة السياسة
- مراجعة سنوية لتحديث السياسات والإجراءات.
- متابعة نتائج التحقيقات والتقارير لضمان التحسين المستمر.
- مجلس الأمناء وفريق القيادة العليا مسؤولون عن التطبيق الفعّال للسياسة.

** :Signed**
Date: ** March 2025 **