

سياسة الأمن الإلكتروني

مقدمة:

على الرغم من أن العالم الرقمي يساعدنا على التواصل ومعرفة المزيد ، إلا أنه أيضًا مكان يمكننا فيه مواجهة السلوك الضار ومن هذا المنطلق كانت ادارة مدرسة البطين العلمية الخاصة حريصة على توعية الطلبة و ذويمهم بإرشادات السلامة الالكترونية- حيث انه من الضروري أن نشرك الجميع في الحوار للحفاظ على سلامتهم وتشجيعهم على تحمل المسؤولية تجاه ما يشاركونه عبر الإنترنت. و لحماية ابنائكم الطلبة بشكل أفضل نحثكم على معرفة المزيد حول الوعي الالكتروني ومراقبة أنشطتهم عبر الإنترنت وفهم إعدادات الخصوصية وتعيينها ووضع قواعد معهم -

الهدف:

1. حماية الطلبة أثناء وجودهم تحت رعاية المدرسة من جميع الأفعال أو جوانب التقصير التي تمثل التنمر
2. رصد و دعم الطلبة الذين يُحتمل أنهم قد تعرضوا لمثل هذه النوع من التنمر

التعريفات:

- الطفل: يعرف الطفل على أنه الفرد الذي يقل عمره عن ثماني عشرة سنة ميلادية.
- حماية الطفل: تعرف بأنها جميع التدابير والخطوات والإجراءات التي يجب إتخاذها لحماية الطلبة من الأخطار التي قد تسبب الضرر أو الإصابة.
- الإساءة: تشمل الإساءة الجسدية، العقاب البدني، الإساءة النفسية، الإساءة الجنسية، كما تشمل كلا من التنمر والإستغلال والإهمال.
- التنمر الإلكتروني: هو ذلك السلوك العدواني غير المرغوب فيه والمتكرر (أو من المحتمل جدا أن يتكرر) لعدة

مرات عن طريق الرسائل الإلكترونية وغرف المحادثة والرسائل النصية والمواقع الإلكترونية أو إرسال الصور والفيديو عن طريق الهواتف المحمولة أو النشر على مواقع الإنترنت. وقد يكون الطالب هو المتسبب بالأذى (المتنمر) أو الضحية أو كلاهما.



• أشكال وطرق التنمر الإلكتروني

1. رسائل كره تصل للطفل.
2. إشاعات وأكاذيب يتم إطلاقها عن الشخص المتنمر عليه.
3. استخدام صور/ مقاطع للشخص بدون أذنه ونشرها دون علمه.
4. انتحال الشخصيات في وسائل التواصل الاجتماعي.
5. موافقة التعليقات السلبية أو المنشورات الكاذبة
6. التهديد بنشر صور / مقاطع / محادثات خاصة.

• علامات التنمر الإلكتروني

1. الرغبة في التوقف عن استخدام الكمبيوتر أو الهاتف المتنقل.
2. الشعور بالقلق أو الترقب عند تلقي رسالة نصية أو بريد إلكتروني.
3. يخفي الطفل الشاشة أو الجهاز عندما يقترب الآخرون -
4. يقوم فجأة بحذف حسابات مواقع التواصل الاجتماعي.
5. تراجع في المستوى الدراسي.
6. يتجنب الطفل المواقف الاجتماعية -
7. ظهور علامات للاكتئاب.
8. تغييرات في المزاج أو السلوك أو قلة النوم أو انعدام شهية الأكل-

أسباب التنمر الإلكتروني

1. الغيرة من الطرف الآخر
2. قد يكون المتنمر ضحية للتنمر من قبل شخص آخر
3. شعور المتنمر بالرغبة في السيطرة على الطرف الآخر
4. محاولة المتنمر تغطية جانب الضعف لديه

السياسة:

1. المدرسة ومديرها يعتبرون كفلاء على حق الطلبة في عدم التعرض للإساءة والإهمال، كما يعد مدير
2. المدرسة موافقاً على القيام بدور ولي الأمر لكل الطلبة أثناء وجودهم تحت رعاية المدرسة وعليه تحمل تبعات هذا الدور.
3. لكافة الطلبة حقوق متساوية في التمتع بالحماية والسلامة

4. تتحمل المدارس المسؤولية الكاملة عن رعاية الطلبة وحمايتهم أثناء وجودهم في رعاية المدرسة
5. يجب أن تضمن المدرسة ايضاً توفير إشراف على الطلبة اثناء استخدام الانترنت-
6. يكون التبليغ عن طريق الهاتف على الخط الساخن (116111)
7. يجب على موظفي المدرسة توعية الطلبة حول أهمية الإبلاغ عن أية حالة إساءة و/أو إهمال

سرية البيانات:

1. تُعتبر تقارير الحالات وبيانات الطلبة حساسة وفي غاية السرية. يجب على جميع الأطراف الذين تتضمنهم الواقعة الحفاظ على سرية الواقعة وسرية هويات الطلبة الذين تعرضوا للإعتداء أو الإهمال المزعوم، والمعتدي المزعوم، والشخص المبلغ عن الحالة المزعومة.
2. يجب عدم الإفصاح عن البيانات سوى للأطراف المخولين من الإدارة المعنية بحماية الطفل بدائرة التعليم و المعرفة ، مركز حماية الطفل وإدارة الدعم الإجتماعي بوزارة الداخلية.
3. يحظر على موظفي المدرسة حضرا تاما مناقشة أي حالات قائمة أو مغلقة مع وسائل الإعلام أو أي أطراف خارجية أخرى أو مع موظفين آخرين، أو مع أي أشخاص غير مخولين من دائرة التعليم و المعرفة باستثناء الجهات التحقيقية والقضائية وفي حدود المسؤولية القانونية.

الادوار والمسؤوليات:

يجب على مديري المدارس القيام بما يلي:

1. الإلتزام بهذه السياسة وإتباع الإجراءات الواردة بها.
2. على مديري المدارس نشر سياسة تعنى بحماية الطلبة من أي إساءة و/أو إهمال على أن تتوافق كحد أدنى مع ما هو منصوص عليه في هذه السياسة ولا تتعارض مع أي من أحكامها.
3. ضمان إتباع موظفي المدارس وقادتها للإجراءات التي قد تحد من حالات الإساءة للطلبة أو إهمالهم، وضمان فهمهم لها.
4. ضمان الإشراف على الطلبة في الأوقات التي يتواجدون فيها تحت رعاية المدرسة.
5. ضمان التركيز والإهتمام الدائم على إعطاء الأولوية القصوى لحماية الطلبة وإتخاذ إجراءات فورية عند الشك في حالات إساءة للطلبة أو إهمالهم.
6. تعزيز قدرة الطلبة على الإبلاغ بأمان عن مخاوفهم بشأن تعرضهم للإساءة و/أو الإهمال دون خوف من التعرض للانتقام أو العقاب.
7. الإطلاع على وجهات نظر الطلبة وأولياء الأمور بشأن الأمن والحماية.

8. الإبلاغ المباشر عن أي حالة إساءة و/أو إهمال محتملة للطلبة
9. التأكد من حضور ومشاركة كافة الموظفين والإداريين بالمدرسة والمستهدفين بتدريب حماية الطفل
10. لكل الحلقات التدريبية.
11. نشر هذه السياسة وتعريف أولياء الامور بأدوارهم ومسؤولياتهم و حقوقهم وواجباتهم.
يتولى جميع موظفي المدرسة ما يلي:

1. الإبلاغ عن أي حالة إساءة و/أو إهمال مُشتبه فيها فور إكتشافها
2. الإشراف الكامل على الطلبة اثناء استخدامهم للانترنت.
يتولى أولياء الامور المسؤوليات التالية:
1. التعاون مع إدارة المدرسة وموظفيها والإجابة على كافة الاستفسارات المتعلقة بسلوك الطالب وأداءه الدراسي والاستجابة لملاحظاتهم وإرشاداتهم.
2. نقل أي تخوفات أو ملاحظات أو تغيرات في سلوك ابنائهم إلى الإدارة المدرسية أو الاخصائي الاجتماعي .
3. مراقب ابنائهم الطلبة في حال ظهرت علامات للتنمر عليهم.
4. توجيه الابناء بحماية كلمات المرور الخاصة بهم والتفاصيل الحسابات على الإنترنت.
5. تعليمهم مفهوم التنمر الإلكتروني وكيفية التعامل معه.
6. تحديد التطبيقات المناسبة لاستخدام ابنائهم الطلبة والغير مناسبة.
7. وضع قواعد حول مقدار الوقت الذي يمكن للطفل إنفاقه على الإنترنت أو على أجهزته.
8. مراقبة مواقع التواصل الاجتماعي والتطبيقات وتاريخ التصفح لابنائهم ، في حال كانت لديه مخاوف من حدوث تنمر إلكتروني له.
9. البقاء على اطلاع دائم على أحدث التطبيقات المستخدمة من قبل الأطفال والمراهقين.
10. التعرف على اسم المستخدم وكلمة المرور الخاصة بالبريد الإلكتروني ووسائل التواصل الاجتماعي لابنائهم.

11. تعزيز ثقة الطفل بنفسه بتجاهل رسائل التنمر الإلكتروني.
12. ابلاغهم بالرجوع اليه أو الى شخص بالغ في حال تعرضهم للتنمر.
يتولى الطلبة المسؤوليات التالية:

1. عدم مشاركة معلوماتهم وتفاصيل حياتهم وعائلته مع الآخرين.
2. حماية الأرقام السرية للحسابات والأجهزة.

3. تكوين علاقات جديدة مع أفراد جيدين.
4. عدم فتح المواقع والرسائل المشبوهة التي يكون هدفها إختراق الأجهزة والحسابات.
5. تسجيل الخروج من حسابه عندما يستخدم أجهزة أخرى غير جهازه.
6. عدم مشاركة معلوماته السرية مع أحد (اسم المستخدم وكلمات المرور)
7. وضع ملصق على الكاميرا الخاصة بجهازه تحسبا للاختراقات.
8. يقوم بحظر أي شخص يحاول استدراجه وتهديده ، حيث ان تجاوبه وردده عليه سيعطيه فرصة للتنمر عليه.
9. التواصل مع والديه وأخوته الكبار في البيت و ادارة المدرسة و الاخصائي الاجتماعي بشكل دائم وفي حال تعرضه لأي شيء مؤذي في الانترنت أبلغهم على الفور-

اقتراحات في حال التعرض للتنمر:

1. لولي الامر

1. تأكد من سلامة طفلك.
2. التحدث مع طفلك والاستماع إليه.
3. جمع الأدلة (قم بتصوير الشاشة أو حفظ الصور التي تثبت التنمر على طفلك)
4. تواصل مع إدارة التطبيق أو البرنامج وأبلغ عن المتنمر.
5. أبلغ عن الحالة للجهات المختصة (وزارة الداخلية /ادارة حماية الطفل/قسم التنمر الإلكتروني)
6. إذا لزم الأمر اذهب بطفلك إلى أخصائي نفسي لمعرفة حالته النفسية.

2. موظفي المدرسة

1. الاستماع إلى الطفل ومحاولة معرفة المشكلة.
2. إبلاغ ادارة المدرسة لالتخاذ الاجراءات المناسبة.
3. تعزيز ثقة الطفل بنفسه بأن لا يتأثر بما يقوله المتنمر.

الاطفال والمراهقين

1. لا ترد فوراً على التنمر الذي تعرضت له ، و لا تتجاوب مع من يهددك أو يبتزك.
2. حجب المتنمر ومنعه من الدخول إلى صفحاتك الخاصة (احذفه من قائمة الأصدقاء وأغلق المحادثة).-
3. الاحتفاظ بالأدلة على التنمر عن طريق التقاط صورة للشاشة -
4. تغيير إعدادات الخصوصية في حسابك (لا تكشف عنوانك أو هاتفك على الإنترنت ، تغيير اسمك المستعار ، إنشاء حساب جديد إذا كنت تخشى أن ينتحل شخصيتك المتنمر)
5. تكلم مع شخص بالغ (والديك أو أخوتك الكبار أو معلمك أو ادارة المدرسة) ، ولا تكتفم ذلك في نفسك.
6. إذا كنت تعرف المتنمر ، اطلب من شخص بالغ التواصل معه لإيقاف التنمر.
7. حاول أن لا تشعر بالخجل من نفسك مهما كان ما نشره أو قاله المتنمر.
8. كن شجاعاً ولا تخجل من طلب المساعدة من الآخرين في حال احتجت لذلك.
9. لا تجعل التعليقات السلبية وتصرفات المتنمرين تؤثر على حياتك الخاصة
10. تعرف على الجهات الرسمية والتي تقدم لك المساعدة لإيقاف التنمر

مرفقات:

خطوات التبليغ عن حالات الإساءة و/أو الإهمال المشتبه بها لطفل:

