Students` Cyber Security Policy	سياسة الأمن الالكتروني للطلاب
Goals Protect students from cyberbullying and teach them how to the face the bullies and how to behave in the event of being cyberbullied in order to maintain a safe learning environment which ensures the cyber and psychological safety of students during the learning process. A Specific policy was developed to evaluate the anticipated risks and measures taken to ensure the continuity of the learning process within a safe environment. **The concept of cyberbullying:** Using means of communication and technologies to intentionally carry out hostile and negative behavior to harm others, such as insulting, threatening violence, defamation, or blackmail, leading to negative consequences such as isolation, fear and failure. **Forms of Cyberbullying: (Potential Risks)** 1- Sending negative messages bearing hatred and racism towards an individual or group of individuals. 2- Distorting the image or reputation of another person by spreading rumors and lies about them. 3- Exploiting an individual's personal affairs, such as using his image, voice, or video clip without his permission, and publishing it without his knowledge. 4- Underestimating or belittling a person. 5- Re-posting offensive comments. 6- Vandalism and piracy in the sense of hacking others` property by sending viruses to them or taking control from them by changing their password or impersonation and stealing the e-mail of the other person while speaking in his name and sending messages on his behalf. 7 – Extortion by threatening the life or reputation of the individual by publishing what is harmful to him if he does not respond to his requests. 8- Impersonation in the media.	**الهدف** **حماية الطلبة من التنمر الإلكتروني و مساعدتهم في مواجهة المتنمرين و كيفية تصرفهم في حالة تعرضهم للتنمر الإلكتروني من أجل الحفاظ على بيئة تعليمية للطلاب خالية من أي معوقات يمكن أن تقف في وجه تحقيق الأمن والسلامة النفسية للطلاب أثناء عملية التعلم الهجين .تم وضع سياسة محددة لتقييم المخاطر المتوقعة والإجراءات المتخذة لضمان استمرارية عملية التعلم ضمن جو بيئي آمن .** **مفهوم التنمر الالكتروني :** **استخدام وسائل تقنيات الاتصال و المعلومات لتنفيذ سلوك عدائي و سلبي بشكل متعمد لإلحاق الأذى بالآخرين كالسب او التهديد بالعنف او التشهير او الابتزاز تؤدي إلى نتائج سلبية مثل الانعزال و الخوف و الفشل .** **أشكال التنمر الإلكتروني : (المخاطر المحتملة)** **1- إرسال رسائل سلبية تحمل الكراهية و العنصرية تجاه فرد أو مجموعة أفراد .** **2- تشويه صورة أو سمعة شخص آخر من خلال الترويج للإشاعات و الأكاذيب عنهم .** **3- استغلال الأمور الشخصية للفرد مثل استخدام صورته أو صوته أو مقطع مرئي بدون الاستئذان منه ونشرها دون علمه .** **4- التقليل من قدر شخص أو تحقيره .** **5- إعادة نشر التعليقات المسيئة .** **6- التخريب والقرصنة بمعنى تخريب ممتلكاته بإرسال فيروسات لهم أو أخذ السيطرة منهم بتغيير الرقم السري الخاص بهم أو إنتحال الشخصية و يقوم بسرق البريد الإلكتروني الخاص بالشخص الآخر مع التحدث بإسمه وإرسال رسائل بالنيابة عنه .** **7- الابتزاز و يكون بتهديد حياة الفرد أو سمعته من خلال نشر ما يضره إن لم يستجب لطلباته .**

8- انتحال الشخصيات في وسائل التواصل .

9- التحرش و هو إرسال صور و رسائل غير مرغوب بها تتسبب في إيذاء مشاعر الشخص الآخر .

10- إخراج الطالب من مجموعة المحادثة و منعه من المشاركة .

11- المضايقات بنشر الطلبة رسائل عدوانية مثل (أنت لست فعال – إجابتك غير صحيحة) ورسائل سلبية تنقص من قيمته المعرفية .

12- المراقبة والمتابعة بمعنى التجسس برصد تحركات الطالب عبر وسائل التواصل الإجتماعي و مراقبته بشكل دائم و سلبي .

الإجراءات التي يجب أن يتبعها الطالب في حالة تعرضه للتنمر الإلكتروني :

1- عدم حذف الرسائل .

2- تجاهل رسالة المتنمر وعدم الرد عليها .

3- التحدث مع والديك عن الحادثة أو التواصل المباشر مع الأخصائية الاجتماعية أو مشرفة القسم لإتخاذ الإجراءات اللازمة وفقا للائحة السلوك المعتمدة من قبل دائرة التعليم و المعرفة .

إجراءات المدرسة مع الشخص المتنمر :

تتبع المدرسة اللائحة السلوكية المتبعة مع حالات التنمر الإلكتروني والذي يعتبر مخالفة من الدرجة الثالثة وهي :

1- اتصال فوري بولي الأمر وإبلاغه بما حدث من الطالب وخصم نصف درجة السلوك الخاصة بمخالفات الدرجة الثالثة .

2- التوجيه الفردي والجمعي للطلاب .

3-في حال تكرار المخالفة خصم الدرجة الكاملة + انعقاد فوري للجنة السلوك +الاتصال بولي الامر وإبلاغه بقرار لجنة السلوك .

3- تتراوح الإجراءات بين تنبيه خطي للطالب إلى سحب حق المستخدم في الدخول و مراقبة الاستخدام لديه .

9- Harassment by sending unwanted pictures and messages that hurt the feelings of the other person.

10- Take the student out of the group and prevent him from participating.

11- Harassment by posting aggressive messages by students such as (You are not effective - your answer is incorrect) and negative messages that diminish others` cognitive value.

12- Monitoring and follow-up in the sense of espionage by monitoring the student's movements through social media, and monitoring him permanently and passively.

Procedures that the student should follow in the case of being exposed to cyberbullying:

1- Do not delete messages.

2- Ignore the bully's message and do not respond to it.

3- Talking with your parents about the accident or directly contacting with the social worker or the department supervisor to take the necessary measures in accordance with the behavior regulations approved by the Department of Education and Knowledge.

School actions with a bully:

The school follows the behavioral regulations of cyberbullying, which is considered a third-degree violation . the regulations are :

1- Immediate contact with the guardian, informing him of what happened from the student, and deducting half of the behavior score for third-degree violations

2- Individual and group guidance for students.

3- In the event of repeating the violation, the full degree will be deducted + immediate meeting of the behavior committee + contacting the guardian and informing him of the behavior committee's decision.

3- The procedures range from a written notice to the student to withdrawing the user's right to enter the online classes and monitoring his use.