



PANCAR NEZİHE ŞAİROĞLU ORTAOKULU E-GÜVENLİK SWOT ANALİZİ

GÜÇLÜ YÖNLER (G) (STRENGTHS)	ZAYIF YÖNLER (Z) (WEAKNESSES)	FIRSATLAR (F) (OPPORTUNITIES)	TEHDİTLER (T) (THREATS)
<p>1. Milli eğitim Bakanlığı tarafından tahsis edilen filtreli (korumalı) internet ağından faydalanmıyoruz.</p> <p>2. EBA destek noktası olan okulumuzda güvenli internet kullanımına Milli Eğitim Bakanlığının destek vermesi.</p> <p>3. Okulumuzun Güvenli İnternet Kullanımı konusu fazlasıyla önemseyen ve bu konuda gerekli önlemleri alan bir kurum olması.</p> <p>4. Okulumuzda cep telefonu, fotoğraf makinesi ve benzeri teknolojik aletlerin izinsiz kullanılmaması ve bu kuralla ilgili görünür uyarı yazılarının bulunması.</p> <p>5. Akademik çalışmayı teşvik edici, yapıcı ve yönlendirici bir yönetim anlayışının olması.</p> <p>6. e-Güvenlik ile ilgili okulumuzda bir komisyonun bulunması ve güvenlik çalışmalarını yürütmesi.</p> <p>7. Bazı öğretmenlerimizin yardımıyla ve kontrolü altında öğrencilere e-güvenlik kurallarına uygun dijital kaynakları kullandırmamız.</p> <p>8. Yeniliklere açık ve gelişen teknolojiye uyum sağlayan, genç, dinamik ve başarılı bir okul kadrosunun olması.</p> <p>9. Teknolojinin okul personeli tarafından yerinde ve doğru bir şekilde kullanılması ve derslere entegre edilmesi.</p> <p>10. Rehberlik servisimizin “Siber zorbalık ve Bilinçli teknoloji kullanımı” ile ilgili öğrenci, öğretmen ve velilere yönelik eğitim ve broşür çalışmalarını yapması.</p>	<p>1. Öğrencilerimizin ailelerinin e-güvenlik yönünden yetersiz kalmaları.</p> <p>2. Güvenli internet kullanımı konusunda yeterli bilgilendirme ve uyarılar yapılmasına rağmen uzaktan eğitim sürecinde takibinin zorlaşması.</p> <p>3. Okulun çevrim içi politikalarının sürekli gelişen teknoloji ve buna paralel olarak ilerleyen dijitalleşmeye ayak uydurmakta zorlanması.</p> <p>4. Okulumuz personelinin bir kısmının yeni teknolojileri ve web 2 araçlarını kullanmada yetersiz kalmaları.</p>	<p>1. Öğrencilerin denetlenmesi açısından güvenlik mağduriyeti yaşanmaması için Milli Eğitimin uzaktan eğitim kanallarının (EBA) kullanılması.</p> <p>2. Okulumuzun E-Safety Label kapsamında eGüvenlik etiketi çalışmalarının yürütülmesi.</p> <p>3. Okul internet sitemizde çeşitli güvenli internet platformlarının öğrencilerimizle ve velilerimizle paylaşılması.</p> <p>4. MEBBİS üzerinden öğretmenler için açılan uzaktan eğitim kurslarının teknoloji kullanımına yönelik artırılması ve faydalandırılması.</p> <p>5. Uzaktan eğitim nedeniyle Rehberlik Servisinin yapacağı çerçeve programa zorunlu olarak “Bilinçli Teknoloji Kullanımının” genel hedef olarak yer almasının eklenmesi.</p> <p>6. Covid-19 süreci sebebiyle öğretmenlerin web 2 araçlarını ve diğer dijital platformları kullanmak zorunda kalması ve böylelikle e-güvenlik kurallarını daha iyi öğrenme çabaları.</p> <p>7. Öğrencilerimize EBA üzerinden siber zorbalık ve e-güvenlik ile ilgili farkındalık yaratmak adına paylaşım yapmıyoruz.</p>	<p>1. Velilerin uzaktan eğitim sebebiyle öğrencilerin ekran bağımlılığının artması konusundaki endişelerinin oluşması.</p> <p>2. Uzaktan eğitim araçlarını yeterli düzeyde kullanmayan eğitimcilerin derslerinin sabote edilmeye açık hale gelmesi.</p> <p>3. İnternet tehditlerinin her geçen gün kendini yenilemesi ve daha cazip hale gelmesi.</p> <p>4. Salgın sürecindeki uzakta eğitimin yaygınlaştığı dönemde zaman zaman İnternet bağlantılarının zayıflaması.</p> <p>5. Öğrencilerin teknoloji imkanlarını olumsuz yönde kullanma ihtimalinin olması.</p> <p>6. Öğrencilerde cep telefonu, bilgisayar kullanma ve televizyon izleme alışkanlığının fazla olması.</p> <p>7. Öğrenciler arasında siber akran zorbalığının yaygınlaşması.</p> <p>8. Öğrencilerin maddi imkansızlıklardan dolayı bilişim aletlerine ve internete yeterince ulaşamaması.</p> <p>9. Sosyal medya ağlarının bilinçsiz ve çok kullanılması sebebiyle güvenlik tehditlerinin artması.</p>



PANCAR NEZİHE ŞAİROĞLU SECONDARY SCHOOL E-SECURITY SWOT ANALYSIS

GÜÇLÜ YÖNLER (G) (STRENGTHS)	ZAYIF YÖNLER (Z) (WEAKNESSES)	FIRSATLAR (F) (OPPORTUNITIES)	TEHDİTLER (T) (THREATS)
<ol style="list-style-type: none">1. To benefit from the filtered (protected) internet network allocated by the Ministry of National Education.2. The support of the Ministry of National Education for the use of safe internet in our school, which is an EBA support point.3. Our school is an institution that attaches great importance to Safe Internet Use and takes the necessary precautions in this regard.4. Not using mobile phones, cameras and similar technological devices without permission in our school and the presence of visible warning letters regarding this rule.5. Having a constructive and directive management approach that encourages academic work.6. There is a commission related to e-Security in our school and it carries out security studies.7. With the help and control of some of our teachers, we allow students to use digital resources in accordance with e-security rules.8. Having a young, dynamic and successful school staff who are open to innovations and adapt to developing technology.9. Using technology in place and correctly by school staff and integrating them into lessons.10. Our guidance service conducts training and brochures for students, teachers and parents on "Cyberbullying and Conscious Technology Use"	<ol style="list-style-type: none">1. Our students' families are insufficient in terms of e-security.2. Despite sufficient information and warnings about safe internet use, it becomes difficult to follow up in the distance education process.3. The difficulty of the school's online policies to keep up with the ever-evolving technology and digitalization progressing in parallel.4. Some of our staff's inability to use new technologies and web 2 tools.	<ol style="list-style-type: none">1. The use of distance education channels (EBA) of National Education in order to prevent security victimization in terms of supervising students.2. Conducting eSafety label studies within the scope of our school's E-Safety Label.3. Sharing various secure internet platforms on our school website with our students and parents.4. Increasing and making use of distance education courses opened for teachers through MEBBİS for the use of technology.5. Adding mandatory "Conscious Use of Technology" to the framework program to be made by the Guidance Service due to distance education.6. Due to the Covid-19 process, teachers have to use web 2 tools and other digital platforms and thus their efforts to learn e-security rules better.7. Sharing our students on EBA to raise awareness about cyberbullying and e-security.	<ol style="list-style-type: none">1. Parents' concerns about the increase in screen addiction of students due to distance education.2. The lessons of educators who do not use distance education tools sufficiently become vulnerable to sabotage.3. Internet threats are constantly improving and becoming more attractive.4. The weakening of Internet connections from time to time during the epidemic period when distance education is becoming widespread.5. Students are likely to use technology opportunities negatively.6. The habit of using mobile phones, computers and watching television among students.7. The widespread use of cyber peer bullying among students.8. Inability of students to access information tools and internet sufficiently due to financial difficulties.9. Security threats increase due to the unconscious and excessive use of social media networks.