



## BELEDİYE ORTAOKULU E-GÜVENLİK SWOT ANALİZİ

GÜÇLÜ YÖNLER	ZAYIF YÖNLER	FIRSATLAR	TEHDİTLER
<p>1.Milli Eğitim Bakanlığı tarafından tahsis edilen filtrelili (korumalı) internet ağından faydalanmamız.</p> <p>2.EBA destek noktası olan okulumuzda güvenli internet kullanımına Milli Eğitim Bakanlığının destek vermesi.</p> <p>3.Okulumuzun Güvenli İnternet Kullanımı konusunu 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 öğretmenler kurulunda alınan karar gereği 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.BT Formatör öğretmenimizin yardımıyla ve kontrolü altında öğrencilere e-güvenlik kurallarına uygun dijital kaynakları kullanılmamamız.</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>11.Okulumuzun dış güvenliğinin MOBESSE kameraları ile sağlanması</p> <p>12.Okul polisi ve okul güvenlik görevlisinin bulunması</p> <p>13.Okulumuzun coğrafi olarak merkezi konumda olması</p> <p>14. Okulumuzda Web2.0 araçlarının kullanılışıyla ilgili öğretmenlere hizmetiçi eğitim verilmesi</p>	<p>1.Öğrencilerimizin ailelerinin e-güvenlik yönünden yetersiz kalmaları.</p> <p>2.Güvenli internet kullanımı konusunda yeterli bilgilendirme ve uyarılar yapılmasına rağmen takibinin zorluğu</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>5.Öğrencilerimizin çoğunluğunun ev ortamında internet ve bilgisayar erişiminin olmayışı</p>	<p>1.Öğrencilerin denetlenmesi açısından güvenlik mağduriyeti yaşanmaması için Milli Eğitimin uzaktan eğitim kanallarının ( EBA) kullanılması.</p> <p>2.Okul internet sitemizde çeşitli güvenli internet platformlarının öğrencilerimizle ve velilerimizle paylaşılması.</p> <p>3.MEBBİS üzerinden öğretmenler için açılan uzaktan eğitim kurslarının teknoloji kullanımına yönelik artırılması ve faydalandırılması.</p> <p>4.Rehberlik Servisinin yapacağı çerçeve programa zorunlu olarak “Bilinçli Teknoloji Kullanımının” genel hedef olarak yer almasının eklenmesi.</p> <p>5.Öğrencilerimize EBA üzerinden siber zorbalık ve e-güvenlik ile ilgili farkındalık yaratmak adına paylaşım yapmamız.</p> <p>6. Okulumuzda ulusal ve uluslar arası e-Twinning projelerinin yürütülmesi</p> <p>7. Okulumuzun Fatih Projesinden yararlanması sayesinde teknolojik donanımlara sahip olması</p> <p>8.Okulumuzda TÜBİTAK Bilim Fuarı yapılması</p> <p>9. Her yıl okulumuzdan TEKNOFEST başvuruları için öğrencilerin yönlendirilmesi</p>	<p>1.Velilerin internet sebebiyle öğrencilerin ekran bağımlılığının artması konusundaki endişelerinin oluşması.</p> <p>2.İnternet tehditlerinin her geçen gün kendini yenilemesi ve daha cazip hale gelmesi.</p> <p>3.Öğrencilerde cep telefonu, bilgisayar kullanma ve televizyon izleme alışkanlığının fazla olması.</p> <p>4.Öğrenciler arasında siber akran zorbalığının yaygınlaşması.</p> <p>5.Öğrencilerin maddi imkansızlıklardan dolayı bilişim aletlerine ve internete yeterince ulaşamaması.</p> <p>6.Sosyal medya ağlarının bilinçsiz ve çok kullanılması sebebiyle güvenlik tehditlerinin artması.</p> <p>7.Öğrencilerin interneti ağırlıklı olarak sosyal medya ve oyunlarla özdeşleştirmeleri</p>