CEMİL MERİÇ FEN LİSESİ

SWOT ANALYSİS

1.1. SWOT Analizi

- Okulumuzda çevrim içi güvenlik hizmetlerini geliştirerek öğrencilerimizi, velilerimizi ve personelimizi her türlü bilinen tehditlerden korumak, onlara karşı önlem almak ve yaşadıkları olumsuzlukları çözmek için strateji geliştirmeleri sağlamak amaçlanmıştır.
- Öğretmenler, okul web sitesi, görüntü ve video paylaşımı, kullanıcılar, içerik,internet ve bilişim cihazları kullanımı, cep telefonu ve kişisel cihaz kullanımı hakkında kurallar belirlenmiştir.

a. Öğretmenler: 1 . e güvenlik politikalarını geliştirmek için yapılan toplantılarda katkı bulunmak
2. e güvenlik konusunda sorumluluk almak
3. Teknolojiyi güvenli olarak kullanmak

4. Zararlı olabilecek durumları gözlemleyip, o anda ise önlemini alıp ilgili birime yönlendirmek
5. https://www.esafetylabel.eu/home sitesinde bloglari ve formlari takip ederek olasi e güvenlik sorunlari ve Çözümleri hakkında bilgilenmek

b. Web sitesi: 1. Web sitesinde adres, telefon,fax ve e-posta adresi bulunmaktadır.
2. Okul web yayın komisyonu tarafından onaylanan resimler yayınlanır.
3. Öğrenci çalışmaları velilerin izniyle yayınlanır.

c. Kullanıcılar: 1. Öğrenciler video hazırlarken video hazırlanmadan önce öğretmenlerinden izin almalıdır
2. Velilerden görüntü öncesi izin alınmalıdır.
3. Video ve konferanslar resmi ve onaylanmış siteler aracılığı ile yapılmalıdır.
4. Şahsi sosyal medya hesaplarında, okul öğrencileri ve çalışanlarının yer aldığı görüntüleri okul web yayın komisyonundan izin almadan yayınlanamaz.
5. Öğrenciler Kabul Edilebilir Kullanım Politikalarına bağlı kalmalıdır.
6. Öğrenciler siber zorbalık veya cinsel içerikli mesajlarla karşılaştıklarında öğretmenlerine veya rehber öğretmenlerine haber vermelerinin gerektiği anlatılır.
7. Öğrenciler kendilerini ve arkadaşlarını siber zorbalıktan ve cinsel içerikli mesajlardan korumaları gerektiği anlatılır.
8. Velilerimiz çocuklarıyla siber zorbalık ve cinsel içerikli mesajlar ile ilgili konuşmalıdır.
9. Velilerimiz öğrencilerimiz egüvenlik sorunlarıyla karşılaştığında öğretmeni veya rehber öğretmeni ile konuşmalıdır.

d. İnternet ve güvenli bilişim cihazlarının kullanımı:
1. İnternet kullanımının bu kadar geniş kitlelere yayılmasından dolayı doğru kullanımını ve siber zorbalık konularını müfredat ile ilişkilendirir.
2. Öğrencilerin ve öğretmenlerin en doğru bilgiye en güvenli şekilde ulaşması sağlanmalıdır.
3. Erişimleri öğrencilerin yaş ve yeteneklerine göre sağlanmıştır.
4. Gerekli filtrelemeler yapılır ve güncellenir.
5. Paydaşlarımız yenilikler hakkında bilgilendirilir.
6. 11. Şubat 2021 güvenli internet günü okulumuzda panolar,yönergeler ve eğitimlerle desteklenir.
7. Ağ güvenlik prosüdürleri uygulanır.

e. Cep telefonu ve kişisel cihaz kullanımı:
1. Öğrencilerin okul saati içinde cep telefonu kullanmaları yasaktır.
2. Okul içinde ve bahçesinde izinsiz toplu fotograf ve video çekimi yapılmamaktadır.
3. Kişisel cihazların sorumluluğu kişilere aittir.
4. İzinsiz yapılan kullanımlardan doğacak olumsuzlukların sorumluluğu kişilere aittir.
5. Çalışanlar telefonları ders saati sırasında sessize almak yada kapatmak zorundadır.

- Okulumuzda paydaşlarımıza güvenli internet hakkında seminerler verilmekte, broşürler dağıtılmaktadır.

- Öğrencilerimize yaşa dışı içerik, siber zorbalık ve cinsel içerikli mesajlasma, ve güvenli internet kullanımı ile ilgili seviyelerine uygun seminerler verilmektedir.

- Okulumuzda web güvenlik komisyonu oluşturulmuştur.

- Öğretmenlerimiz https://www.esafetylabel.eu/home 'a üye olmuş, oradaki yenilikleri, gelişmeleri, blogları ve kaynakları takip etmektedir. Bunun dışında http://etwinningonline.eba.gov.tr/ web sitesinden "İnternet Güvenliği ve e Twinning Etiği" ile "eSafety Label Hakkında Herşey" eğitimlerini alarak güncel bilgileri takip etmektedir.

- Okulumuzda yaşanacak herhangi bir olumsuzluk durumunda ilk başta olayı fark eden öğretmenimiz gerekli önlemleri alıp, durumu web güvenlik komisyonuna bildirmelidir.

	Faydalı	**Zararlı** to achieving your strategy
İç Faktörler	*Güçlü Yönler* 1Öğretmenlerin egüvenlik konusunda ilgili olması 2. Öğretmenlerin teknolojiyi etkin kullanması 3. Okulumuzda teknoloji bakımından yeterli olması 4. Okulumuzda müfredatlarımızda e güvenlik konusunun işlenmesi 5. Öğrenci profilinin iyi olması 6. Okulumuz da kantin ve yemekhane öğrencilerimiz ve öğretmenlerimize hizmet sunmaktadır. 7. Belediye ile işbirliği yapılmaktadır. 8. Okulumuzda Kabul Edilebilir Kullanım Politikasının olması	*Zayıf Yönler* 1. Velilerin egüvenlik hakkında bilgilerinin olmaması 2. Okulumuz sınavla öğrenci aldığı için farklı şehirlerden öğrenciler bulunuyor ve bu öğrenciler okul pansiyonunda kalıyorlar. Bundan dolayı velilerimizi egüvenlik ile ilgili bilgilendirme seminerlerine katılamayabiliyorlar. 3. Velilerin sosyoekonomik durumunun zayıf olması 4. Öğremenlerin hizmet içi eğitime katılım oranın düşük olması
External factors **(Aspects outside the control of your school)**	*Fırsatlar* 1. Milli Eğitim Bakanlığı'nın e güvenlik ile ilgili kendı filtreleme sisteminin olması Çevrim içi filteleme sisteminin okul bilgisayarlarımızda yüklü olması ve sürekli güncellenmesi 3.Öğrencilerin yaşları uygun olduğu için seminerler daha etkili ve verimli oluyor.	*Tehditler* 1. Öğretmenlerimizin kişisel bilgisayarlarının yeterli çevrim içi güvenlik kaynaklarının olmaması 2.Öğrencilerin sosyoekonomik düzeyi yüksek olmadığı için güvenliği yüksek antivürüs??? 3.Velilerimizin eğitim düzeyinin düşük olması