



BAHÇELİEVLER İLKOKULU

Bahçelievler İlkokulu e-Güvenlik Komisyonu Kasım 2023

İÇİNDEKİLER

İÇİNDEKİLER	1
YÖNERGELER.....	2
1. OKUL ORTAMINI ANLAMA.....	2
Okul Tanımı.....	2
Okulun Misyonu Ve Görevi.....	2
Okulun Değerleri	2
SWOT Analizi.....	2
2. ÇEVİRİM İÇİ GÜVENLİK STRATAJİSİNİ TANIMLAMA	5
Strateji Vizyonu	5
Odak Noktası	5
Stratejik Hedefler ve Amaçlar	5
Çevrimiçi Güvenlik Stratejisini Yürütme	6
Hareket Planı	6

YÖNERGELER

Bu belge Elazığ Bahçelievler İlkokulu 2023-2024 e-Güvenlik stratejik planı olarak hazırlanmıştır.

1. OKUL ORTAMINI ANLAMA

Okul Tanımı

Elazığ il merkezinde yer alan okulumuz 6950 m²'lik okul alanı üzerine 470 m²'lik kapalı alana sahip okulumuzun 13 derslik, ve çok amaçlı salonu ile kütüphanesi mevcuttur.

Okulun Misyonu Ve Görevi

Okulumuzun misyonu, Atatürk İlkeleri ışığında, nitelikli eğitim alan, pozitif ilimlerle donatılmış, her alanda başarıyı hedefleyen, ulusal ve evrensel değerlere saygıyı ilke edinen, demokratik bireyler yetiştirmek için varız...

Okulun Değerleri

- Tüm paydaşlarımızı çevrimiçi olarak korumak ve güvenliklerini sağlamak
- Teknolojinin potansiyel riskleri ve yararları konusunda tüm paydaşların farkındalığını sağlamak
- Güvenli internet kullanırken tüm olumlu davranışları <https://www.esafetylevel.eu/home> da online modellemek ve kendi standartlarını ve uygulamalarını yürütme gereksinimini fark etmek
- Her türlü bilinen çevrimiçi güvenlik sorunlarına yanıt verebilecek prosedürleri tanımlamak

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 geliştirmelerini 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. eGüvenlik 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.esafetylevel.eu/home> sitesinde blogları ve formları takip ederek olası e güvenlik sorunları ve çözümleri hakkında bilgilenecek

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

- ### c. Kullanıcılar:
1. Öğrenciler video hazırlarken 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 görüntüler okul web yayın komisyonundan izin almadan yayınlanamaz.
 5. Öğrenciler Kabul Edilebilir Kullanım Politikalarına bağlı kalmalıdır.
 6. Öğrencilere siber zorbalık veya cinsel içerikli mesajlarla karşılaştıklarında öğretmenlerine veya rehber öğretmenlerine bilgi vermeleri gerektiği anlatılır.
 7. Öğrencilere kendilerini ve arkadaşlarını siber zorbalıktan ve cinsel içerikli mesajlardan korumaları gerektiği anlatılır.
 8. Velilerimiz çocuklarıyla siber zorbalık ve cinsel içerikli mesajlar ile ilgili bilgi paylaşımında bulunmalıdır.
 9. Velilerimiz, öğrencilerimiz e-Güvenlik sorunlarıyla karşılaştığında öğretmeni veya rehber öğretmeni ile iletişim kurmalıdır.

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 "Güvenli İnternet Günü" okulumuzda kutlanır.
7. Ağ güvenlik prosedürleri uygulanır.

e. Cep telefonu ve kişisel cihaz kullanımı:

1. Öğrencilerin okul saati içinde cep telefonu kullanmaları yasaktır.
2. Okul içinde ve bahçesinde izinsiz toplu fotoğraf 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.

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

- ❖ Öğrencilerimize yaşadışı içerik, siber zorbalık ve cinsel içerikli mesajlaşma, çocuk istismarı hakkında 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 HakkındaHerşey" eğitimlerini alarak güncel bilgileri takip etmektedirler.
- ❖ Okulumuzda yaşanacak herhangi bir olumsuzluk durumunda ilk başta olayı fark eden öğretmenimiz gerekli önlemleri alıp, durumu web güvenlik komisyonuna bildirmektedir.

İç Faktörler	<i>Güçlü Yönler</i> 1. Öğretmenlerin eGüvenlik konusunda ilgili olması 2. Öğretmenlerin teknolojiyi etkin kullanması 3. Okulumuzun teknoloji bakımından yeterli olması 4. Okulumuzda müfredatlarımızda e güvenlik konusunun işlenmesi 5. Okulumuzda Kabul Edilebilir Kullanım Politikasının olması	<i>Zayıf Yönler</i> 1. Velilerin e güvenlik hakkında yeterli bilgivedonanımasahipolmamaları
	<i>Fırsatlar</i> 1. Milli Eğitim Bakanlığı'nın e güvenlik ile ilgili kendi filtreleme sisteminin olması 2. Çevrim içi filtreleme sisteminin okul bilgisayarlarımızda yüklü olması ve sürekli güncellenmesi 3. Öğrencilerinin yaşlarının küçük olması okulda öğretmenlerinin gözetiminde teknolojiyi kullanması.	<i>Tehditler</i> 1. Öğretmenlerimizin kişisel bilgisayarlarının yeterli çevrim içi güvenlik kaynaklarının olmaması 2. Öğrencilerin yaş grubunun küçük olması ve bu yüzden tehditlerin farkında olmaması
External factors (Aspects outside the control of your school)		

2. ÇEVİRİM İÇİ GÜVENLİK STRATAJİSİNİ TANIMLAMA

Strateji Vizyonu

Okulumuz, teknolojik aletleri kullanırken çocukları ve yetişkinleri dijital dünyanın zararlarından korumaktır. Bunun için gerekli çalışmalar yapılmaktadır. Sanal platformların ve bilgi iletişim teknolojilerinin vazgeçilmez hale geldiğini görülmektedir. Çocuklarımızı bu ortamlardan gelebilecek riskleri yönetmeleri, bu risklere nasıl tepki vermeleri konusunda strateji geliştirmenin yollarını öğrenmeleri amaçlanmıştır. Personelimizin mesleki çalışmalarını desteklemek, başarıyı teşvik etmek ve yönetim işlevlerini geliştirmek için internet erişimi sunma yükümlülüğü verilmiştir. Bütün paydaşlarımızı (velilerimizi, öğrencilerimizi ve personelimizi) sanal ortamdan korunmasını sağlama misyonumuzdur.

Odak Noktası

- Sosyal medya ile ilgili riskler konusunda okul farkındalığının artırılması
- e Güvenliğin öneminin farkına varılması
- Öğrencilerimizi siberzorbaliğa, cinsel içerikli mesajlara karşı korunması ve strateji geliştirilmesinin sağlanması
- Personelin kendi e Güvenliği hakkında bilgilendirilmesi

Stratejik Hedefler ve Amaçlar

Odak Noktası	Stratejik Hedefler	Amaçlar
Sosyal Medya	1.1 Sosyal medya ile ilgili riskler konusunda okul farkındalığını 1 yıl içinde %40' a çıkartmak.	1.1.1 2024 yılının sonuna kadar velilerimizin sosyal medya ile ilgili riskler konusunda farkındalığının artırılması.
		1.1.2 2024 yılının sonuna kadar öğrencilerimizin sosyal medya ile ilgili riskler konusunda farkındalığının artırılması.
		1.1.3 2024 yılının sonuna kadar personelimizin sosyal medya ile ilgili riskler konusunda farkındalığının artırılması.
Güvenli internet eğitimi	1.2 eGüvenliğin öneminin okul farkındalığını 1 yıl içinde %40' a çıkartmak.	1.2.1 2024 sonuna kadar velilerimize e güvenlik konusunda bilgilendirme yapmak
		1.2.2 2024 yılının sonuna kadar öğrencilerimizin e Güvenlik konusunda farkındalığının artırılması
		1.2.3 2024 yılının sonuna kadar personelimizin e Güvenlik konusunda farkındalığının artırılması.

Siber Zorbalık	1.3 Öğrencilerin siber zorbalığa ve cinsel içerikli mesajlara karşı korunması ve strateji geliştirmesini %40' a çıkartmak	1.3.1 2024 yılının sonuna kadar öğrencilerimizin siber zorbalığa ve cinsel içerikli mesajlara karşı korunma ve strateji geliştirmesinin artırılması.
		1.3.2 2024 yılının sonuna kadar velilerimizin siber zorbalığa ve cinsel içerikli mesajlara karşı korunma ve strateji geliştirmesinin artırılması.
		1.3.3 2024 yılının sonuna kadar personellerimizin siber zorbalığa ve cinsel içerikli mesajlara karşı korunma ve strateji geliştirmesinin artırılması.
Personel Eğitimi	2.1 Personelin kendini güvenliğini hakkında bilgilendirilmesinin bir yılda %40 çıkartmak.	2.1.1 2024 yılının sonuna kadar personelimizin https://www.esafetylabel.eu/home a üye olmasını sağlamak
		2.1.2 2024 yılının sonuna kadar personelimizin http://etwinningonline.eba.gov.tr/ da eğitimleri almasını sağlamak

Çevrimiçi Güvenlik Stratejisini Yürütme Hareket Planı

HEDEF	ETKİNLİK	YETKİLİ KİŞİ	SÜRE	HEDEFLENEN SONUÇ	KULLANILAN ARAÇ
2024 yılının sonuna kadar velilerimize sosyal medya ile ilgili riskler konusunda okul farkındalığının artırılması.	Seminerler vermek		MAR RT 20 24	1 saat içinde velilere sosyal medyada karşılaşılabilecek ile riskler le ilgili bilgilendirme	Bilgisayar Akıllı Tahta https://www.guvenliweb.org.tr/
		Web güvenlik komisyonu	Şubat 2024	11.Şubat.2024 güvenli internet gününde sosyal medya ile ilgili riskler bilgilendirme	
2024 yılının sonuna kadar öğrencilerimize sosyal medya ile ilgili riskler konusunda okul farkındalığının artırılması.	Seminerler vermek		MAR T 2024	1 saat içinde öğrencilere sosyal medya ile riskler konusunda bilgilendirme	Bilgisayar Akıllı Tahta https://www.guvenliweb.org.tr/
	Panolar hazırlamak	Sınıf Rehber öğretmenleri	Şubat 2024	11.Şubat.2024 güvenli internet gününde sosyal medya ile ilgili riskler bilgilendirme	

HEDEF	ETKİNLİK	YETKİLİ KİŞİ	SÜRE	HEDEFLenen SONUÇ	KULLANILAN ARAÇ
2024 sonuna kadar velilerimize sınıf öğretmenleri tarafından e güvenlik konusunda bilgilendirme yapma	Seminerler vermek		MAR T 2024	1 saat içinde e güvenlik konusunda bilgilendirme	Bilgisayar Akıllı Tahta https://www.guvenliweb.org.tr/
2024 sonuna kadar öğrencilerimize sınıf öğretmenleri tarafından e güvenlik konusunda bilgilendirme yapma	Seminerler vermek		MAR T 2024	1 saat içinde öğrencilere sosyal medya ile riskler konusunda bilgilendirme	Bilgisayar Akıllı Tahta https://www.guvenliweb.org.tr/
	Panolar hazırlamak	Sınıf Rehber öğretmenleri	Şubat 2024	11.Şubat.2024 güvenli internet gününde panoda ilgili paylaşımlar yapma	
2024 sonuna kadar personelimize sınıf öğretmenleri tarafından e güvenlik konusunda bilgilendirme yapma	Seminerler vermek https://www.esafetylabel.eu/home		MAR T 2024		Bilgisayar Akıllı Tahta https://www.guvenliweb.org.tr/

