



Ticaret Borsası İlkokulu

e-Güvenlik Komisyonu 2023

İÇİNDEKİLER

| | |
|---|---|
| İÇİNDEKİLER..... | 1 |
| YÖNERGELER | 2 |
| 1. OKUL ORTAMINI ANLAMA | 2 |
| 1.1. Okul Tanımı | 2 |
| 1.2. Okulun Misyonu Ve Görevi | 2 |
| 1.3. Okulun Değerleri..... | 2 |
| 1.4. SWOT Analizi | 2 |
| 2. ÇEVİRİM İÇİ GÜVENLİK STRATAJİSİNİ TANIMLAMA | 5 |
| 2.1. Strateji Vizyonu..... | 5 |
| 2.2. Odak Noktası | 5 |
| 2.3. Stratejik Hedefler ve Amaçlar..... | 5 |
| Çevrimiçi Güvenlik Stratejisini Yürütme..... | 6 |
| 2.4. Hareket Planı | 6 |
| 3. İlerlemeyi İzleme ve Çevrimiçi Güvenlik Stratejisini Değerlendirme | 8 |
| 4. Risk Değerlendirmesi..... | 9 |



YÖNERGELER

Bu belge web güvenlik komisyonu tarafından Eskişehir Tepebaşı Ticaret Borsası İlkokulu'nun 2022-2023 e güvenlik stratejik planı olarak hazırlanmıştır.

1. OKUL ORTAMINI ANLAMA

1.1. Okul Tanımı

Ticaret Borsası İlkokulu, Batıkent mahallesi, Eskişehir ili Türkiye' dedir. Okulumuzun hedef grubu ilkokuldur. 996 öğrencisi bulunmaktadır. 26 ilkokul, 4 anasınıfımız mevcuttur. Okulumuzda 34 öğretmen, 1 müdür, 2 müdür yardımcısı ve 2 memur görev yapmaktadır.

1.2. Okulun Misyonu

MİSYON

Çevre bilinci kazanmış, sosyal uyum sağlayan, etik değerlere sahip; mutlu, özgür ve kendine güvenen bireyler yetiştirmektir.

VİZYON

Yenilikleri yakalayan, sürekli gelişimi ilke edinmiş, işbirlikçi, tüm çalışanların liderlik yapabildiği ve güvenli internet kullanımının olduğu örnek bir okul olmak.

1.3. Okulun Değerleri

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

1.4. 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.esafetylabel.eu/home> sitesinde blogları ve formları takip ederek olası e güvenlik sorunları ve Çözümleri hakkında bilgilenmek
- 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 görüntüleri okul web yayın komisyonundan izin almadan yayınlanamaz.
 5. Öğrenciler Kabul Edilebilir Kullanım Politikasına bağlı kalmalıdır.
 6. Öğrenciler siber zorbalık veya cinsel içerikli mesajlarla karşılaştıklarında öğretmenlerine veya rehber öğretmenlerine gelmeleri 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 kullanılır.
 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 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.
- ❖ Okulumuzda paydaşlarımıza güvenli internet hakkında seminerler verilmekte, broşürler dağıtılmaktadır.
- ❖ Öğrencilerimize yaşa dışı içerik, siber zorbalık ve cinsel içerikli mesajlaşma, çocuk istismarı hakkında seviyelerine uygun seminerler verilmektedir.
- ❖ Okulumuzda web güvenlik komisyonu oluşturulmuştur.

- ❖ Öğretmenlerimiz <https://www.esafetylevel.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 | <p><i>Güçlü Yönler</i></p> <ol style="list-style-type: none"> 1. Öğretmenlerin egüvenlik konusunda ilgili olması 2. Öğretmenlerinteknolojiyi etkin kullanması 3. Okulumuzda teknoloji bakımından yeterli olması 4. Okulumuzda müfredatımızda e güvenlik konusunun işlenmesi 5. Okulumuzda Kabul Edilebilir Kullanım Politikasının olması | <p><i>Zayıf Yönler</i></p> <ol style="list-style-type: none"> 1. Velilerin egüvenlik hakkında bilgilerinin olmaması 2. Sürekli göç alan bir okul olunmasından dolayı veli profilinin sürekli değişmesi 3. Velilerin sosyoekonomik durumunun zayıf olması |
| External factors (Aspects outside the control of your school) | <p><i>Fırsatlar</i></p> <ol style="list-style-type: none"> 1. Milli Eğitim Bakanlığı'nın e güvenlik ile ilgili kendi filtreleme sisteminin olması 2. Çevrim içi filteleme sisteminin okul bilgisayarlarımızda yüklü olması ve sürekli güncellenmesi 3. Öğrencilerinin yaşlarının küçük olması okulda öğretmenlerinin gözetiminde teknolojiyi kullanması. | <p><i>Tehditler</i></p> <ol style="list-style-type: none"> 1. Öğretmenlerimizin kişisel bilgisayarlarının yeterli çevrim içi güvenlik kaynaklarının olmaması 2. Öğrencilerin yaş grubunun küçük olması ve bu yüzden tehditlerin farkında olmaması 3. Velilerimizin eğitim düzeyinin düşük olması |

2. ÇEVİRİM İÇİ GÜVENLİK STRATAJİSİNİ TANIMLAMA

2.1. 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.

2.2. Odak Noktası

1. Sosyal medya ile ilgili riskler konusunda okul farkındalığının artması
2. Egüvenliğin öneminin farkına varılması
3. Öğrencilerimizi siber zorbalığa, cinsel içerikli mesajlara karşı korunması ve strateji geliştirilmesinin sağlanması
4. Personelin kendi e güvenliği hakkında bilgilendirilmesi

2.3. Stratejik Hedefler ve Amaçlar

| Odak Noktası | Stratejik Hedefler | Amaçlar |
|----------------------------------|---|---|
| Odak Notası | 1.1 Sosyal medya ile ilgili riskler konusunda okul farkındalığının 1 yıl içinde %10'a çıkartmak. | <p>1.1.1 2023 yılının sonuna kadar velilerimize sosyal medya ile ilgili riskler konusunda okul farkındalığının arttırılması.</p> <p>1.1.2 2023 yılının sonuna kadar öğrencilerimize sosyal medya ile ilgili riskler konusunda okul farkındalığının arttırılması</p> <p>1.1.3 2023 yılının sonuna kadar personelimize sosyal medya ile ilgili riskler konusunda okul farkındalığının arttırılması.</p> |
| 1Güvenli internet eğitimi | 1.2 egüvenliğin öneminin okul farkındalığını 1 yıl içinde %10 a çıkartmak | <p>1.2.1 2023 sonuna kadar velilerimize e güvenlik konusunda bilgilendirme yapma</p> <p>1.2.2 2023 yılının sonuna kadar öğrencilerimize e güvenlik konusunda okul farkındalığının arttırılması</p> <p>1.2.3 2023 yılının sonuna kadar personelimize e güvenlik konusunda okul farkındalığının arttırılması</p> |

| | | |
|----------|--|---|
| Personel | 1.3 Öğrencilerin siber zorbalığa ve cinsel içerikli mesajlara karşı korunması ve strateji geliştirmesini %10 a çıkartmak | 1.3.1 2023 yılının sonuna kadar öğrencilerimize siber zorbalığa ve cinsel içerikli mesajlara karşı korunması ve strateji geliştirmesini arttırılması. |
| | | 1.3.2 2023 yılının sonuna kadar velilerimize siber zorbalığa ve cinsel içerikli mesajlara karşı korunması ve strateji geliştirmesini arttırılması. |
| | | 1.3.3 2023 yılının sonuna kadar personellerimize siber zorbalığa ve cinsel içerikli mesajlara karşı korunması ve strateji geliştirmesini arttırılması. |
| Personel | 2.1 Personelin kendini güvenliğini hakkında bilgilendirilmesinin bir yılda %10 a çıkartmak. | 2.1.1 2023 yılının sonuna kadar personelimizi https://www.esafetylabel.eu/home a üye olmasını sağlamak |
| | | 2.1.2 2023 yılının sonuna kadar personelimizi http://etwinningonline.eba.gov.tr/ da eğitimleri almasını sağlamak |

Çevrimiçi Güvenlik Stratejisini Yürütme

2.4. Hareket Planı

| Amaç | Activite | Sorumlu Kişi | Zaman Dilimi | Beklenen Sonuç/Girdi | Araçlar |
|--|--------------------------------------|------------------------|--------------|--|--|
| Amaç 1.1.1 2023 yılının sonuna kadar velilerimize sosyal medya ile ilgili riskler konusunda okul farkındalığının arttırılması. | Seminerler vermek | Derya BAYAR | Ocak 2023 | 1 saat içinde velilere sosyal medya ile riskler konusunda bilgilendirme | Bilgisayar Projeksiyon https://www.guvenliweb.org.tr/ |
| | Broşurler vermek | Web güvenlik komisyonu | Şubat 2023 | 11.Şubat.2021 güvenli internet gününde sosyal medya ile ilgili riskler bilgilendirme | https://www.guvenliweb.org.tr/ |
| Amaç 1.1.2 2023 yılının sonuna kadar öğrencilerimize sosyal medya ile ilgili riskler konusunda okul farkındalığının arttırılması. | Seminerler vermek | Tuğba Gökmen | Ocak 2023 | 1 saat içinde öğrencilere sosyal medya ile riskler konusunda bilgilendirme | Bilgisayar Projeksiyon https://www.guvenliweb.org.tr/ |
| | Broşurler vermek, panolar hazırlamak | Sınıf öğretmenleri | Şubat 2023 | 11.Şubat.2021 güvenli internet gününde sosyal medya ile ilgili riskler bilgilendirme | https://www.guvenliweb.org.tr/ |

| | | | | | |
|--|---|--------------------|------------|--|---|
| <p>Amaç 1.1.3</p> <p>2023 yılının sonuna kadar personelimize sosyal medya ile ilgili riskler konusunda okul farkındalığının artırılması .</p> | Seminerler vermek | Tuğba Gökmen | Ocak 2023 | 1 saat içinde personellerimize sosyal medya ile riskler konusunda bilgilendirme | Bilgisayar Projeksiyon https://www.guvenliweb.org.tr/ |
| <p>Amaç 1.2.1</p> <p>2023 sonuna kadar velilerimize sınıf öğretmenleri tarafından e güvenlik konusunda bilgilendirme yapma.</p> | Seminerler vermek | Fatih ÖZEN | Ocak 2023 | 1 saat içinde e güvenlik konusunda bilgilendirme | Bilgisayar Projeksiyon https://www.guvenliweb.org.tr/ |
| <p>Amaç 1.2.2</p> <p>2023 yılının sonuna kadar öğrencilerimize e güvenlik konusunda okul farkındalığının artırılması.</p> | Broşurler vermek, | Sınıf öğretmenleri | Şubat 2023 | 11.Şubat.2023 güvenli internet gününde sosyal medya ile ilgili riskler bilgilendirme | https://www.guvenliweb.org.tr/ |
| <p>Amaç 1.2.3</p> <p>2023 yılının sonuna kadar personelimize e güvenlik konusunda okul farkındalığının artırılması.</p> | Seminerler vermek | Fatih ÖZEN | Ocak 2021 | 1 saat içinde e güvenlik konusunda bilgilendirme | Bilgisayar Projeksiyon https://www.guvenliweb.org.tr/ |
| <p>Amaç 1.2.3</p> <p>2023 yılının sonuna kadar personelimize e güvenlik konusunda okul farkındalığının artırılması.</p> | https://www.esafetylebel.eu/home | Kendisi | Yıl içinde | https://www.esafetylebel.eu/home üye olarak e güvenlik hakkında güncel verileri takip etmek | Bilgisayar |
| <p>Amaç 1.3.1</p> <p>2023 yılının sonuna kadar öğrencilerimize siber zorbalığa ve cinsel içerikli mesajlara karşı korunması ve strateji geliştirmesini artırılması.</p> | Seminer | Sınıf öğretmenleri | Subat 2021 | 1 saat içinde siber zorbalığa ve cinsel içerikli mesajlara karşı korunması konusunda bilgilendirme | Bilgisayar Projeksiyon https://www.guvenliweb.org.tr/ |
| <p>Amaç 1.3.2</p> <p>2023 yılının sonuna kadar velilerimize siber zorbalığa ve cinsel içerikli mesajlara karşı</p> | Müfredatin içinde işlemek | Sınıf öğretmenleri | Yıl içinde | Yıl içinde derslerde bu konu ile ilgili bilgilendirme, drama yapma | Web siteleri |
| <p>Amaç 1.3.2</p> <p>2023 yılının sonuna kadar velilerimize siber zorbalığa ve cinsel içerikli mesajlara karşı</p> | Seminer vermek | Sınıf öğretmenleri | Yıl içinde | Yıl içinde veli toplantılarında bu konu ile ilgili bilgilendirme yapma | Web siteleri |



| | | |
|---|--|---|
| <p>korunması ve strateji geliştirmesini arttırılması.</p> <p>Amaç 1.3.3</p> <p>2023 yılının sonuna kadar personellerimize siber zorbalığa ve cinsel içerikli mesajlara karşı korunması ve strateji geliştirmesini arttırılması için seminerler vermek.</p> | <p>Seminer vermek</p> <p><i>Sevim Dalyan</i></p> <p><i>Şubat 2023</i></p> <p><i>1 saat içinde siber zorbalığa ve cinsel içerikli mesajlara karşı korunması konusunda bilgilendirme</i></p> | <p><i>Bilgisayar Projeksiyon</i></p> <p>https://www.guvenliweb.org.tr/</p> |
| <p>Amaç 2.1.1</p> <p>2023 yılının sonuna kadar personelimizi https://www.esafetylabel.eu/home a üye olmasını sağlamak</p> | <p>Öğretmenler kurul toplantısı</p> <p><i>kendisi</i></p> <p><i>Yıl içinde</i></p> <p><i>Yıl içerisinde https://www.esafetylabel.eu/home a üye olması ve blogları takip etmesini sağlamak</i></p> | <p>https://www.esafetylabel.eu/home</p> |
| <p>Amaç 2.1.3</p> <p>2023 yılının sonuna kadar personelimizi http://etwinningonline.eba.gov.tr/ da eğitimleri almasını sağlamak</p> | <p>Öğretmenler Kurul toplantısı</p> <p><i>Kendisi</i></p> <p><i>Nisan 2023</i></p> <p><i>Nisan ayındaki yapılacak olan ara tatilde kursları almak.</i></p> | <p>http://etwinningonline.eba.gov.tr/</p> <p><i>“İnternet Güvenliği ve e Twinnin Etiği” ile “eSafety Label Hakkında Herşey” eğitimleri</i></p> |

3. İlerlemeyi İzleme ve Çevrimiçi Güvenlik Stratejisini Değerlendirme

| Odak Noktası | Stratejik Amaç | İlerleme Yada Amaç Nasıl Değerlendirilecek? | Zaman Aralığı |
|---|--|--|---|
| Odak Noktası1 <i>güvenli internet</i> | 1.1 Sosyal medya ile ilgili riskler konusunda okul farkındalığının 1 yıl içinde %10 a çıkartmak. | Anketler yapılması ve web.güvenlik komisyonu tarafından belgelendirilmesi | Zaman1: Eylül 2022 Zaman2: Haziran 2023 |
| | 1.2 e-güvenliğin öneminin okul farkındalığını 1 yıl içinde%10 a çıkartmak | Anketler yapılması ve web güvenlik komisyonu tarafından belgelendirilmesi | Survey 1: Eylül 2022 Survey 2: Haziran 2023 |
| | 1.3 Öğrencilerin siber zorbalığa ve cinsel içerikli mesajlara karşı korunması ve strateji geliştirmesini %10 a çıkartmak | Anketler yapılması ve web güvenlik komisyonu tarafından belgelendirilmesi. Sınıf öğretmenlerinin ve rehber öğretmenlerinin bu konu ile ilgili yaptığı görüşmeler ve gözlemler yıl sonunda değerlendirilmesi | Survey 1: Ocak 2023 Survey 2: Haziran 2023 |
| Personel | 2.1 Personelin kendini egüvenliğini hakkında bilgilendirilmesinin bir yılda %10 a çıkartmak. | https://www.esafetylevel.eu/home a üyelik ve http://etwinningonline.eba.gov.tr/ "İnternet Güvenliği ve e Twinning Etiği" ile "eSafety Label Hakkında Herşey" eğitimlerinin sertifikaları | Zaman1: Ocak 2023 Zaman2: Haziran 2023 |

4. Risk Değerlendirmesi

| Güvenlik Açısından Potansiyel riskler | Belirlenen Potansiyel Riskler Nasıl Hafifletilir? |
|---|---|
| 1. Öğrencinin kişisel bilgilerinin çalınması | <ul style="list-style-type: none"> - Öğrencinin öğretmenine bildirmesi - Öğrencinin rehber öğretmen ile görüşmesinin sağlanması - Rehber öğretmenle birlikte sınıf öğretmenin veliye bu konu hakkında bilgilendirmesi ve nesil önlemler alabileceği hakkında görüşme yapılması - Öğretmenin web güvenlik komisyonuna bildirmesi. - Okul polisine haber verilmesi |
| 2. Öğrencinin öğretmenin açık olan bilgisayarından e okul'a girip bütün notların değiştirilmesi | <ul style="list-style-type: none"> - Öğretmenin bilgisayarına şifre koyması - Sınıftan çıkarken bilgisayarını kapatması veya uyku moduna alması - Şifresini herhangi bir yere yazmaması - Şifrelerini 3 ayda bir değiştirmesi |
| 3. Öğrencilerin okul internet ağı kullanıcı şifresinin öğrenciler tarafından keşfedilmesi | <ul style="list-style-type: none"> - Velilerimizi uygun bir dille bunun yanlış olduğunu anlatılır. - Uzun şifrelerin belirlenmesi - Şifrelerde büyük küçük harf, sayı ve noktalama işaretlerinin kullanılarak zorluk seviyesini arttırmak - Şifrelerin 3 ayda bir değiştirilmesi |