FIRAT ANADOLU LİSESİ

E GÜVENLİK BELGESİ 2025

İÇİNDEKİLER

YÖNERGELER

Bu belge web güvenlik komisyonu tarafından Fırat Anadolu Lisesi 2024-2025 e güvenlik stratejik planı olarak hazırlanmıştır.

1. OKUL ORTAMINI ANLAMA

1.1 Okul Tanımı

Fırat Anadolu Lisesi Lisesi Çayda Çıra mahallesi, Merkez ilçesi, Elazığ ili Türkiye' dedir. Okulumuzun hedef grubu lisedir.
Okulumuzun 675 öğrencisi bulunmaktadır. Okulumuzda 31 derslik ,1 fen, 1 kimya, 1 biyoloji,2 müzik, 2 görsel sanatlar derslikleri, 1 bilgisayar laboratuarı,1 yemekhanesi mevcuttur. Okulumuzda 63 öğretmen, 1 müdür, 2 müdür yardımcısı ve 2 memur görev yapmaktadır.

OKULUMUZUN MİSYONU

Öğretmenlerimizin yetenekleri dikkate alınarak, hayat boyu; * Bilgili, * Kültürlü, * Becerikli, Özgüvenli, Problemlerin çözümünde bilimsel yöntemleri kullanan, * Bilgi ve iletişim teknolojilerinde uzmanlaşmış, * Uluslararası bilince sahip, * İş birliği ve ekip çalışmalarına yatkın lider gençler yetiştirmektir.

Okulun Misyonu Ve Görevi
Teknolojiyi yakından takip eden, değişime ve yeniliğe açık, kültürünü ve değerlerini yaşayan ve yaşatan, hoşgörü sahibi, farklılıkları zenginlik kabul eden en az bir yabancı dil bilen sosyal ve kültürel faaliyetlere katılımcı, kendini sorgulayan, farkındalığı ve topluma faydalı bir birey olma bilinci yüksek, etkili ve nitelikli bireyler yetiştirmektir

1.1. Okulun e Güvenlik Değerleri

1. Okulmuzun tüm paydaşlarını çevrimiçi olarak korumak ve güvenliklerini sağlamak
2. Teknolojinin potansiyel riskleri ve yararları konusunda tüm paydaşların farkındalığını sağlamak
3. Güvenli internet kullanırken tüm olumlu davranışları ve siber güvenlik ile ilgili bilgilendirmeleri arttırmak ve kendi standartlarını ve uygulamalarını yürütme gereksinimini fark etmek
4. Her türlü bilinen çevrimiçi güvenlik sorunlarına yanıt verebilecek prosadürleri tanımlamak

1.4. SWOT Analizi

Amaç:

Okulumuzda çevrim içi güvenlik hizmetlerini geliştirerek; öğrencilerimizi, velilerimizi ve personelimizi bilinen tehditlerden korumak, bu tehditlere karşı önlem almak ve yaşanabilecek olumsuzlukları çözmek için stratejiler geliştirmek temel hedefimizdir.

Genel Kurallar:

Öğretmenler, okul web sitesi, görüntü ve video paylaşımı, kullanıcılar, internet ve bilişim cihazları kullanımı, cep telefonu ve kişisel cihaz kullanımı gibi konulara yönelik belirli kurallar oluşturulmuştur.

a. Öğretmenler:

1. Okulun e-güvenlik politikalarının geliştirilmesi amacıyla düzenlenen toplantılara aktif katılım sağlamak.
2. e-Güvenlik ile ilgili sorumluluklarını eksiksiz yerine getirmek.
3. Teknolojiyi güvenli ve etkili bir şekilde kullanmak.
4. Zararlı olabilecek durumları gözlemleyerek anında müdahale etmek ve ilgili birime bildirmek.
5. eSafety Label platformundaki blog ve forumları takip ederek e-güvenlik sorunları ve çözümleri hakkında bilgi edinmek.

b. Web Sitesi:

1. Okulun iletişim bilgileri (adres, telefon, faks ve e-posta) web sitesinde açıkça yer alır.
2. Web sitesinde yalnızca okul web yayın komisyonu tarafından onaylanan görseller paylaşılır.
3. Öğrenci çalışmaları, velilerden alınan izin doğrultusunda yayınlanır.

c. Diğer Kullanıcılar:

1. Öğrenciler, herhangi bir görüntü kaydı almadan önce okul idaresinden ve öğretmenlerinden izin almalıdır.
2. Veliler, öğrencilerin görüntü kayıtları için önceden yazılı izin vermelidir.
3. Video konferans ve benzeri etkinlikler yalnızca resmi ve güvenilir platformlar üzerinden gerçekleştirilmelidir.
4. Kişisel sosyal medya hesaplarında, okul öğrencileri ve çalışanlarının yer aldığı görüntüler, okul web yayın komisyonundan izin alınmadan paylaşılamaz.
5. Öğrenciler, **Kabul Edilebilir e Güvenlik Kullanım Politikaları**'na uymakla yükümlüdür.
6. Öğrenciler, siber zorbalık veya cinsel içerikli mesajlarla karşılaştıklarında öğretmenlerine veya rehber öğretmenlerine bilgi vermelidir.
7. Siber zorbalık ve cinsel içerikli mesajlardan korunma konusunda öğrencilere, okul rehberlik servisi veya sınıf rehber öğretmenleri tarafından bilgilendirme yapılır.
8. Veliler, çocuklarıyla siber zorbalık ve cinsel içerikli mesajlar hakkında düzenli olarak konuşmalıdır.
9. Veliler, öğrencilerin e-güvenlik sorunlarıyla karşılaştığında öğretmen veya rehber öğretmenle iletişime geçmelidir.

d. İnternet ve Güvenli Bilişim Cihazları Kullanımı:

1. İnternetin yaygın kullanımı göz önünde bulundurularak, doğru internet kullanımı ve siber zorbalık konuları müfredata entegre edilir.
2. Öğrencilerin ve öğretmenlerin en doğru bilgiye güvenli şekilde ulaşmaları sağlanır.
3. İnternet erişimi, öğrencilerin yaş ve gelişim seviyelerine uygun olarak düzenlenir.
4. Gerekli filtreleme sistemleri uygulanır ve düzenli olarak güncellenir.
5. Tüm paydaşlar, teknolojik yenilikler ve güvenlik önlemleri hakkında bilgilendirilir.

6. **13 Şubat Güvenli İnternet Günü**, okul genelinde pano, yönerge ve eğitimlerle desteklenir.
7. Ağ güvenlik prosedürleri titizlikle uygulanır.

e. Cep Telefonu ve Kişisel Cihaz Kullanımı:

1. Öğrencilerin okul saatleri içinde cep telefonu kullanmaları yasaktır.
2. Okul içinde ve bahçede izinsiz toplu fotoğraf ve video çekimi yapılmaz.

3. Kişisel cihazların sorumluluğu tamamen kullanıcıya aittir.
4. İzinsiz kullanımlardan kaynaklanan olumsuzlukların sorumluluğu kullanıcıya aittir.
5. Çalışanlar, ders saatleri boyunca telefonlarını sessize almak veya kapatmak zorundadır.

Diğer Faaliyetler:
- Okulumuzda paydaşlarımıza yönelik güvenli internet kullanımı seminerleri düzenlenmekte ve bilgilendirici broşürler dağıtılmaktadır.
- Öğrencilerimize yaşa uygun içeriklerle siber zorbalık, cinsel içerikli mesajlaşma ve güvenli internet kullanımı konularında seminerler verilmektedir.
- Okulumuzda web güvenlik komisyonu oluşturulmuş olup, bu komisyon güvenlik politikalarının uygulanmasını denetlemektedir.

- Okulumuzda öğretmenlerimiz gönüllü olarak https://www.esafetylabel.eu/home 'a üye olmuş, oradaki yenilikleri, gelişmeleri, blogları ve kaynakları takip etmektedir. Bunun dışında European School Education Platform | European School Education Platform
- 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 e güvenlik olumsuzluk durumunda ilk başta olayı fark eden öğretmenimiz gerekli
  önlemleri alıp, durumu web güvenlik komisyonuna bildirmelidir.

İç Faktörler

Güçlü Yönler:

1. **Öğretmenlerin e-Güvenlik Konusunda Bilinçli ve İlgili Olması:**
   Öğretmenlerimiz, e-güvenlik konularına karşı duyarlıdır ve bu alanda kendilerini sürekli geliştirmektedir. Bu durum, öğrencilerin dijital güvenliği konusunda etkili bir rehberlik sağlamaktadır.
2. **Öğretmenlerin Teknolojiyi Etkin ve Verimli Kullanması:**
   Öğretmenlerimiz, teknolojik araçları derslerinde etkin bir şekilde kullanarak öğrencilerin dijital becerilerini geliştirmektedir. Bu durum, eğitim-öğretim süreçlerinin daha verimli hale gelmesine katkıda bulunmaktadır.
3. **Okulumuzun Teknolojik Altyapı Açısından Yeterli Olması:**
   Okulumuz, teknolojik donanım ve altyapı bakımından yeterli düzeydedir. Bu durum, öğrencilerin ve öğretmenlerin teknolojiden en üst düzeyde faydalanmasını sağlamaktadır.
4. **Müfredatımızda e-Güvenlik Konularının Yer Alması:**
   Okulumuzda e-güvenlik konuları müfredata entegre edilmiştir. Bu sayede öğrenciler, dijital dünyada karşılaşabilecekleri risklere karşı bilinçlendirilmektedir.

5. **Öğrenci Profilinin Başarılı ve Uyumlu Olması:**
   Öğrencilerimiz, akademik ve sosyal açıdan başarılı bir profile sahiptir. Bu durum, e-güvenlik konularına daha kolay adapte olmalarını ve bu konularda sorumluluk almalarını kolaylaştırmaktadır.
6. **Kantin ve Yemekhane Hizmetlerinin Sunulması:**
   Okulumuzda öğrencilerimize ve öğretmenlerimize yönelik kantin ve yemekhane hizmetleri bulunmaktadır. Bu hizmetler, okulda geçirilen zamanın daha konforlu ve verimli olmasını sağlamaktadır.

Zayıf Yönler:

1. Velilerin e-Güvenlik Konusunda Bilgi Eksikliği:
   Velilerimizin büyük bir kısmı, e-güvenlik konuları hakkında yeterli bilgiye sahip değildir. Bu durum, öğrencilerin evdeki dijital güvenliğini olumsuz etkileyebilmektedir.

2. Öğrenciler ve Velilerin Seminerlere Katılım Zorluğu:
   Okulumuz sınavla öğrenci aldığı için farklı şehirlerden gelen öğrenciler bulunmaktadır. Bu öğrenciler okul pansiyonunda kalmakta ve velileri e-güvenlik seminerlerine katılamamaktadır. Bu durum, velilerin bilinçlendirilmesi önünde bir engel oluşturmaktadır.

3. Velilerin Sosyoekonomik Durumunun Zayıf Olması:
   Velilerimizin bir kısmının sosyoekonomik durumu zayıftır. Bu durum, öğrencilerin teknolojik imkanlara erişimini kısıtlayabilmekte ve e-güvenlik konularında eksikliklere neden olabilmektedir.

4. Öğretmenlerin Hizmet İçi Eğitimlere Katılım Oranının Düşük Olması
   Öğretmenlerimizin hizmet içi eğitimlere katılım oranı düşüktür. Bu durum, e-güvenlik ve teknoloji kullanımı konularında güncel bilgilerin yaygınlaşmasını engelleyebilmektedir.

Bu analiz, okulumuzun e-güvenlik alanındaki güçlü ve zayıf yönlerini ortaya koymakta ve bu alanda yapılacak iyileştirmeler için bir temel oluşturmaktadır. İçerik aynı kalırken ifadeler biraz daha detaylandırılarak ve farklı bir anlatım tarzıyla sunulmuştur

Fırsatlar

1• **Milli Eğitim Bakanlığı'nın kendi filtreleme sistemine sahip olması**, e-güvenlik açısından önemli bir avantajdır.
2• **Çevrim içi filtreleme sisteminin okul bilgisayarlarına yüklü olması ve düzenli olarak güncellenmesi**, güvenli internet kullanımını desteklemektedir.
3• **Öğrencilerin yaşlarına uygun olması nedeniyle**, verilen seminerler daha etkili ve verimli hale gelmektedir.

Tehditler

1• **Öğretmenlerin kişisel bilgisayarlarında yeterli çevrim içi güvenlik kaynaklarının bulunmaması**, dijital güvenliği olumsuz etkileyebilmektedir.
2• **Öğrencilerin sosyoekonomik düzeyinin düşük olması nedeniyle**, güvenlik seviyesi yüksek antivirüs programlarına erişimleri sınırlı olabilmektedir.
3• **Velilerin eğitim düzeyinin düşük olması**, dijital güvenlik konularında farkındalık eksikliğine yol açabilmektedir.

2. ÇEVRİM İÇİ GÜVENLİK STRATAJİSİNİ TANIMLAMA

2.1. Strateji Vizyonu

Okulumuzda, teknolojik ve sanal araçları kullanırken gençleri ve yetişkinleri dijital dünyanın zararlarından korumak için önlemler alınır ve bunun için gerekli çalışmalar yapılmaktadır. Sanal platformların ve bilgi iletişim teknolojilerinin vazgeçilmez hale geldiği görülmektedir. Öğrencilerimizi 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 hedefimizdir.

2.2 Odak Noktası

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

2.1. Stratejik Hedefler ve Amaçlar

1.1 Sosyal medya ile ilgili riskler konusunda okul farkındalığını **artırmak.**

- **1.1.1** 2025 yılının sonuna kadar velilerimizin sosyal medya riskleri konusundaki farkındalığını artırmak.
- **1.1.2** 2025 yılının sonuna kadar öğrencilerimizin sosyal medya riskleri konusundaki farkındalığını artırmak.
- **1.1.3** 2025 yılının sonuna kadar personelimizin sosyal medya riskleri konusundaki farkındalığını artırmak.

1.2 E-güvenliğin önemine dair okul farkındalığını **artırmak.**

- **1.2.1** 2025 yılının sonuna kadar velilerimize e-güvenlik konusunda bilgilendirme yapmak.
- **1.2.2** 2025 yılının sonuna kadar öğrencilerimizin e-güvenlik konusundaki farkındalığını artırmak.
- **1.2.3** 2025 yılının sonuna kadar personelimizin e-güvenlik konusundaki farkındalığını artırmak.

2.1 Personelin e-güvenlik konusunda bilinçlendirilmesini **artırmak.**

- **2.1.1** 2025 yılının sonuna kadar personelimizin eSafety Label platformuna üye olmasını teşvik etmek.
- **2.1.2** 2025 yılının sonuna kadar personelimizin eTwinning Online platformunda eğitim almasını sağlamak.

❖ 2.1.3 2025 yılının sonuna kadar personelimizinEuropean School Education Platform | European School Education Platformuna sağlamak

3.Risk Değerlendirmesi

Güvenlik Açısından Potansiyel Riskler	Belirlenen Potansiyel Riskleri Hafifletme Yöntemleri
1. Öğrencinin kişisel bilgilerinin çalınması	- Öğrencinin durumu sınıf rehber öğretmenine bildirmesi sağlanır. - Öğrencinin rehber öğretmenle görüşmesi teşvik edilir. - Rehber öğretmen ve sınıf öğretmeni, veliyi bilgilendirerek alınabilecek önlemler hakkında görüşme yapar. - Öğretmen, konuyu web güvenlik komisyonuna iletir. - Gerekli durumlarda okul polisine haber verilir.
2. Öğrencinin öğretmenin açık bilgisayarından e-Okul'a girerek notları değiştirmesi	- Öğretmen bilgisayarına güçlü bir şifre koymalıdır. - Sınıftan çıkarken bilgisayarını kapatmalı veya uyku moduna almalıdır. - Şifresini herhangi bir yere yazmamalıdır. - Şifrelerini her 3 ayda bir değiştirmelidir.
3. Öğrencilerin okul internet ağı kullanıcı şifresini keşfetmesi	- Velilere bu durumun sakıncaları uygun bir dille anlatılmalıdır. - Daha karmaşık ve uzun şifreler belirlenmelidir. - Şifrelerde büyük-küçük harf, rakam ve noktalama işaretleri kullanılarak güvenlik seviyesi artırılmalıdır. - Şifreler her 3 ayda bir değiştirilmelidir.

Güvenlik Açısından Potansiyel Riskler ve Nasıl Hafifletilir?

1. **Öğrencinin kişisel bilgilerinin çalınması**
   - Öğrencinin durumu sınıf rehber öğretmenine bildirmesi sağlanır.
   - Öğrencinin rehber öğretmen ile görüşmesi teşvik edilir.
   - Rehber öğretmen ve sınıf öğretmeni, veliyi bilgilendirerek alınacak önlemler hakkında görüşme yapar.
   - Öğretmen, durumu web güvenlik komisyonuna bildirir.
   - Okul polisine haber verilir.
2. **Öğrencinin öğretmenin açık bilgisayarından e-Okul'a girip notları değiştirmesi**
   - Öğretmen bilgisayarına güçlü bir şifre koyar.
   - Sınıftan çıkarken bilgisayarını kapatır veya uyku moduna alır.
   - Şifresini herhangi bir yere yazmaz.
   - Şifrelerini her 3 ayda bir değiştirir.
3. **Öğrencilerin okul internet ağı kullanıcı şifre belirleme kuralları**
   - Velilere şifrelerin başkalarına verilmesinin yanlış olduğu uygun bir şekilde anlatılır.
   - Uzun ve karmaşık şifreler belirlenir.
   - Şifrelerde büyük-küçük harf, rakam ve noktalama işaretleri kullanılarak güvenlik seviyesi artırılır.
   - Şifreler her 3 ayda bir değiştirilir.

Co-funded by the
Erasmus+ Programme
of the European Union