



# Ağcagüney İmam Hatip Ortaokulu

Ağcagüney İmam Hatip Ortaokulu e-Güvenlik Komisyonu Eylül 2021

# 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
3. İlerlemeyi İzleme ve Çevrimiçi Güvenlik Stratejisini Değerlendirme .....	8
4. Risk Değerlendirmesi .....	9



# YÖNERGELER

Bu belge web güvenlik komisyonu tarafından Çarşamba Ağcagüney İmam Hatip Ortaokulu'nun 2022 - 2022 e-güvenlik stratejik planı olarak hazırlanmıştır.

## 1.OKUL ORTAMINI ANLAMA

### Okul Tanımı

Ağcagüney Ortaokulu, Yukarı Ağcagüney Mahallesi, Samsun ili Çarşamba ilçesi Türkiye' dedir. Okulumuzun hedef grubu orta okuldur. 60 öğrencisi bulunmaktadır. Okulumuzda 10 öğretmen, 1 müdür, 1 müdür yardımcısı görev yapmaktadır.

### Okulun Misyonu Ve Görevi

Okulumuzun misyonu, Atatürkçü düşünmeye sahip, nitelikli kendine ve topluma saygı duyan, hedefleri olan eleştirel düşünme yetisine sahip, teknolojiyi verimli kullanabilen ve onun zararlarına karşı strateji geliştirebilen, geleceğe umutla bakan öğrenciler yetiştirmektir.

### 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 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. 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 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 hazırlanamadan 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 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 e-güvenlik 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. 2022 güvenli internet günü okulumuzda kullanılır.
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.

- ❖ 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
<b>İç Faktörler</b>	<p><i>Güçlü Yönler</i></p> <p>1. Öğretmenlerin e-güvenlik konusunda ilgil olması</p> <p>2. Öğretmenlerin teknolojiyi etkin kullanması</p> <p>3. Okulumuzda teknoloji bakımından yeterli olması</p> <p>4. Okulumuzda müfredatlarımızda e güvenlik konusunun işlenmesi</p> <p>5. Okulumuzda Kabul Edilebilir Kullanım Politikasının olması</p>	<p><i>Zayıf Yönler</i></p> <p>1. Velilerin e-güvenlik hakkında bilgilerinin olmaması</p> <p>2. Sürekli göç alan bir okul olunmasından dolayı veli profilinin sürekli değişmesi</p> <p>3. Velilerin sosyoekonomik durumunun zayıf olması</p>
<b>External factors (Aspects outside the control of your school)</b>	<p><i>Fırsatlar</i></p> <p>1. Milli Eğitim Bakanlığı'nın e güvenlik ile ilgili kendi filtreleme sisteminin olması</p> <p>2. Çevrim içi filtreleme sisteminin okul bilgisayarlarımızda yüklü olması ve sürekli güncellenmesi</p> <p>3. Öğrencilerinin yaşlarının küçük olması okulda öğretmenlerinin gözetiminde teknolojiyi kullanması.</p>	<p><i>Tehditler</i></p> <p>1. Öğretmenlerimizin kişisel bilgisayarlarının yeterli çevrim içi güvenlik kaynaklarının olmaması</p> <p>2. Öğrencilerin yaş grubunun küçük olması ve bu yüzden tehditlerin farkında olmaması</p> <p>3. Velilerimizin eğitim düzeyinin düşük olması</p>

## 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

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

### Stratejik Hedefler ve Amaçlar

Odak Noktası	Stratejik Hedefler	Amaçlar
<b>Odak Notası</b>	<b>1.1</b> Sosyal medya ile ilgili riskler konusunda okul farkındalığının 1 yıl içinde %10 a çıkartmak.	<p>1.1.1 2022 yılının sonuna kadar velilerimize sosyal medya ile ilgili riskler konusunda okul farkındalığının arttırılması.</p> <p>1.1.2 2022 yılının sonuna kadar öğrencilerimize sosyal medya ile ilgili riskler konusunda okul farkındalığının arttırılması</p> <p>1.1.3 2022 yılının sonuna kadar personelimize sosyal medya ile ilgili riskler konusunda okul farkındalığının arttırılması.</p>
<b>1Güvenli internet eğitimi</b>	<b>1.2</b> egüvenliğin öneminin okul farkındalığını 1 yıl içinde %10 a çıkartmak	<p>1.2.1 2022 sonuna kadar velilerimize e güvenlik konusunda bilgilendirme yapma</p> <p>1.2.2 2022 yılının sonuna kadar öğrencilerimize e güvenlik konusunda okul farkındalığının arttırılması</p> <p>1.2.3 2022 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 2022 yılının sonuna kadar öğrencilerimize siber zorbalığa ve cinsel içerikli mesajlara karşı korunması ve strateji geliştirmesini arttırılması.
		1.3.2 2022 yılının sonuna kadar velilerimize siber zorbalığa ve cinsel içerikli mesajlara karşı korunması ve strateji geliştirmesini arttırılması.
		1.3.3 2022 yılının sonuna kadar personellerimize siber zorbalığa ve cinsel içerikli mesajlara karşı korunması ve strateji geliştirmesini arttırılması.
Personel	2.1 Personelin kendini e-güvenliğini hakkında bilgilendirilmesinin bir yılda %10 a çıkartmak.	2.1.1 2022 yılının sonuna kadar personelimizi <a href="https://www.esafetylebel.eu/home">https://www.esafetylebel.eu/home</a> a üye olmasını sağlamak
		2.1.2 2022 yılının sonuna kadar personelimizi <a href="http://etwinningonline.eba.gov.tr/">http://etwinningonline.eba.gov.tr/</a> da eğitimleri almasını sağlamak

## Çevrimiçi Güvenlik Stratejisini Yürütme

### Hareket Planı

Amaç	Activite	Sorumlu Kişi	Zaman Dilimi	Beklenen Sonuç/Girdi	Araçlar
Amaç 1.1.1 2022 yılının sonuna kadar velilerimize sosyal medya ile ilgili riskler konusunda okul farkındalığının arttırılması.	Seminerler vermek	Eser KORKMAZ	Ocak 2022	1 saat içinde velilere sosyal medya ile riskler konusunda bilgilendirme	Bilgisayar Akıllı Tahta <a href="https://www.guvenliweb.org.tr/">https://www.guvenliweb.org.tr/</a>
	Broşurler vermek	Web güvenlik komisyonu	Şubat 2022	08.Şubat.2022güvenli internet gününde sosyal medya ile ilgili riskler bilgilendirme	<a href="https://www.guvenliweb.org.tr/">https://www.guvenliweb.org.tr/</a>
Amaç 1.1.2 2022 yılının sonuna kadar öğrencilerimize sosyal medya ile ilgili riskler konusunda okul farkındalığının arttırılması.	Seminerler vermek	Eser KORKMAZ	Ocak 2022	1 saat içinde öğrencilere sosyal medya ile riskler konusunda bilgilendirme	Bilgisayar Akıllı Tahta <a href="https://www.guvenliweb.org.tr/">https://www.guvenliweb.org.tr/</a>
	Broşurler vermek, panolar hazırlamak	Sınıf öğretmenleri	Şubat 2022	08.Şubat.2022güvenli internet gününde sosyal medya ile ilgili riskler bilgilendirme	<a href="https://www.guvenliweb.org.tr/">https://www.guvenliweb.org.tr/</a>

<b>Amaç 1.1.3</b> 2022 yılının sonuna kadar personelimize sosyal medya ile ilgili riskler konusunda okul farkındalığının artırılması .	Seminerler vermek	Eser KORKMAZ	Ocak 2022	1 saat içinde personellerimize sosyal medya ile riskler konusunda bilgilendirme	Bilgisayar Akıllı Tahta <a href="https://www.guvenliweb.org.tr/">https://www.guvenliweb.org.tr/</a>
<b>Amaç 1.2.1</b> 2022 sonuna kadar velilerimize sınıf öğretmenleri tarafından e güvenlik konusunda bilgilendirme yapma.	Seminerler vermek	Eser KORKMAZ	Ocak 2022	1 saat içinde e güvenlik konusunda bilgilendirme	Bilgisayar Akıllı Tahta <a href="https://www.guvenliweb.org.tr/">https://www.guvenliweb.org.tr/</a>
<b>Amaç 1.2.2</b> 2022 yılının sonuna kadar öğrencilerimize e güvenlik konusunda okul farkındalığının artırılması.	Broşurler vermek,	Sınıf Öğretmenleri web güvenlik komisyonu	Şubat 2022	08.Şubat.2022güvenli internet gününde sosyal medya ile ilgili riskler bilgilendirme	<a href="https://www.guvenliweb.org.tr/">https://www.guvenliweb.org.tr/</a>
<b>Amaç 1.2.3</b> 2022 yılının sonuna kadar personelimize e güvenlik konusunda okul farkındalığının artırılması.	Seminerler vermek	Sınıf öğretmenleri	Şubat 2022	1 saat içinde e güvenlik konusunda bilgilendirme	Bilgisayar Akıllı Tahta <a href="https://www.guvenliweb.org.tr/">https://www.guvenliweb.org.tr/</a>
<b>Amaç 1.2.3</b> 2022 yılının sonuna kadar personelimize e güvenlik konusunda okul farkındalığının artırılması.	Pano hazırlamak	Sınıf öğretmenleri	Şubat 2022	08.Şubat.2022güvenli internet gününde pano hazırlama	Güvenli internet günü ile ilgili afişler ve resimler
<b>Amaç 1.3.1</b> 2022 yılının sonuna kadar öğrencilerimize siber zorbalığa ve cinsel içerikli mesajlara karşı korunması ve strateji geliştirmesini artırılması.	Seminer vermek	Eser KORKMAZ	Ocak 2022	1 saat içinde e güvenlik konusunda bilgilendirme	Bilgisayar Akıllı Tahta <a href="https://www.guvenliweb.org.tr/">https://www.guvenliweb.org.tr/</a>
<b>Amaç 1.3.2</b> 2022 yılının sonuna kadar velilerimize siber zorbalığa ve cinsel içerikli mesajlara karşı	<a href="https://www.esafetylebel.eu/home">https://www.esafetylebel.eu/home</a>	Kendisi	Yıl içinde	<a href="https://www.esafetylebel.eu/home">https://www.esafetylebel.eu/home</a> üye olarak e güvenlik hakkında güncel verileri takip etmek	Bilgisayar
<b>Amaç 1.3.1</b> 2022 yılının sonuna kadar öğrencilerimize siber zorbalığa ve cinsel içerikli mesajlara karşı korunması ve strateji geliştirmesini artırılması.	Seminer	Sınıf öğretmenleri	Subat 2022	1 saat içinde siber zorbalığa ve cinsel içerikli mesajlara karşı korunması konusunda bilgilendirme	Bilgisayar Akıllı Tahta <a href="https://www.guvenliweb.org.tr/">https://www.guvenliweb.org.tr/</a>
<b>Amaç 1.3.1</b> 2022 yılının sonuna kadar öğrencilerimize siber zorbalığa ve cinsel içerikli mesajlara karşı korunması ve strateji geliştirmesini artırılması.	Müfredatin içinde işlemek	Sınıf öğretmenleri	Yıl içinde	Yıl içinde derslerde bu konu ile ilgili bilgilendirme, drama yapma	Web siteleri
<b>Amaç 1.3.2</b> 2022 yılının sonuna kadar velilerimize siber zorbalığa ve cinsel içerikli mesajlara karşı	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><b>Amaç 1.3.3</b></p> <p>2022 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>Şubat 2022</i></p> <p><i>1 saat içinde siber zorbalığa ve cinsel içerikli mesajlara karşı korunması konusunda bilgilendirme</i></p> <p><i>Bilgisayar Akıllı Tahta</i></p> <p><a href="https://www.guvenliweb.org.tr/">https://www.guvenliweb.org.tr/</a></p>				
<p><b>Amaç 2.1.1</b></p> <p>2022 yılının sonuna kadar personelimizi <a href="https://www.esafetylabel.eu/home">https://www.esafetylabel.eu/home</a> a üye olmasını sağlamak</p>	<p>Öğretmenler kendisi</p> <p>Yıl içinde</p> <p><i>Yıl içerisinde</i></p> <p><a href="https://www.esafetylabel.eu/home">https://www.esafetylabel.eu/home</a> a üye olması ve blogları takip etmesini sağlamak</p> <p><a href="https://www.esafetylabel.eu/home">https://www.esafetylabel.eu/home</a></p>				
<p><b>Amaç 2.1.3</b></p> <p>2022 yılının sonuna kadar personelimizi <a href="http://etwinningonline.eba.gov.tr/">http://etwinningonline.eba.gov.tr/</a> da eğitimleri almasını sağlamak</p>	<p>Öğretmenler Kendisi</p> <p>Nisan 2022</p> <p><i>Nisan ayındaki yapılacak olan ara tatilde kursları almak.</i></p> <p><a href="http://etwinningonline.eba.gov.tr/">http://etwinningonline.eba.gov.tr/</a></p> <p>“İnternet Güvenliği ve e Twinnin Etiği” ile “eSafety Label Hakkında Herşey” eğitimleri</p>				

### 3. İlerlemeyi İzleme ve Çevrimiçi Güvenlik Stratejisini Değerlendirme

Odak Noktası	Stratejik Amaç	İlerleme Yada Amaç Nasıl Değerlendirilecek?	Zaman Aralığı
<b>Odak Noktası1</b> <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 2020 Zaman2: Haziran 2022
	1.2 e-güvenliğin öneminin okul farkındalığını 1 yıl içinde%10 a çıkartmak	Anketler yapılması ve web güvenlik komisyonu tarafından belgelendirilmesi	Survey 1: Eylül 2020 Survey 2: Haziran 2022
	1.3 Öğrencilerin siber zorbalığa ve cinsel içerikli mesajlara karşı korunması ve strateji geliştirmesini %10a ıkartmak	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 2022 Survey 2: Haziran 2022
<b>Personel</b>	2.1 Personelin kendini e-güvenliğini hakkında bilgilendirilmesinin bir yılda %10 a çıkartmak.	<a href="https://www.esafetylevel.eu/home">https://www.esafetylevel.eu/home</a> a üyelik ve <a href="http://etwinningonline.eba.gov.tr/">http://etwinningonline.eba.gov.tr/</a> "İnternet Güvenliği ve e Twinning Etiği" ile "eSafety Label Hakkında Herşey" eğitimlerinin sertifikaları	Zaman1: Ocak 2022 Zaman2: Haziran 2022

## 4. Risk Değerlendirmesi

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