



LÜLEBURGAZ ATATÜRK İLKOKULU

Lüleburgaz Atatürk İlkokulu e-Güvenlik Komisyon Raporu
EKİM 2020

İÇİNDEKİLER

İÇİNDEKİLER.....	1
YÖNERGELER.....	3
1. ÇEVİRİM İÇİ GÜVENLİK STRATEJİSİNİ TANIMLAMA.....	3
1.1. Strateji Vizyonu.....	3
1.2. Odak Noktası.....	3
1.3. Stratejik Hedefler ve Amaçlar.....	4
2. ÇEVİRİM İÇİ GÜVENLİK STRATEJİSİNİ YÜRÜTME.....	5
2.1. Hareket Planı.....	5
3. İlerlemeyi İzleme ve Çevrim İçi Güvenlik Stratejisini Değerlendirme.....	7
4. Risk Değerlendirmesi.....	8



This project has received funding from the European Union.
This communication reflects only the author's view. It does not represent the view of the European Commission and the EC is not responsible for any use that may be made of the information it contains.

YÖNERGELER

Bu belge web güvenlik komisyonu tarafından Lüleburgaz Atatürk İlkokulu'nun 2020-2021 e güvenlik stratejik planı olarak hazırlanmıştır.

2. ÇEVİRİM İÇİ GÜVENLİK STRATEJİSİNİ 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. e-Güvenliğin öneminin farkına varılması
3. Öğrencilerimizin siber zorbalığa, cinsel içerikli mesajlara, teknoloji bağımlılığına 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 Notası1 Güvenli internet eğitimi	1.1 Sosyal medya ile ilgili riskler konusunda okul farkındalığının 1 yıl içinde %10 a çıkarmak.	1.1.1 2021 yılının sonuna kadar velilerimize sosyal medya ile ilgili riskler konusunda okul farkındalığının arttırılması. 1.1.2 2021 yılının sonuna kadar öğrencilerimize sosyal medya ile ilgili riskler konusunda okul farkındalığının arttırılması 1.1.3 2021 yılının sonuna kadar personelimize sosyal medya ile ilgili riskler konusunda okul farkındalığının arttırılması
	1.2 güvenliğin öneminin okul farkındalığını 1 yıl içinde %10 a çıkarmak	1.2.1 2021 yılı sonuna kadar velilerimize e güvenlik konusunda bilgilendirme yapma 1.2.2 2021 yılının sonuna kadar öğrencilerimize e güvenlik konusunda okul farkındalığının arttırılması. 1.2.3 2021 yılının sonuna kadar personelimize e güvenlik konusunda okul farkındalığının arttırılması
	1.3 Öğrencilerin siber zorbalığa, cinsel içerikli mesajlara ve teknoloji bağımlılığına karşı korunması ve strateji geliştirmesini %10 a çıkarmak	1.3.1 2021 yılının sonuna kadar öğrencilerimizin siber zorbalığa, cinsel içerikli mesajlara ve teknoloji bağımlılığına karşı korunması ve strateji geliştirmesinin arttırılması. 1.3.2 2021 yılının sonuna kadar velilerimizin siber zorbalığa, cinsel içerikli mesajlara ve teknoloji bağımlılığına karşı korunması ve strateji geliştirmesinin arttırılması. 1.3.3 2021 yılının sonuna kadar personellerimizin siber zorbalığa ve cinsel içerikli mesajlara karşı korunması ve strateji geliştirmesinin arttırılması.
Personel	2.1 Personelin kendi güvenliği hakkında bilgilendirilmesinin bir yılda %10 a çıkarmak.	2.1.1 2021 yılının sonuna kadar personelimizi https://www.esafetylabel.eu/home a üye olmasını sağlamak 2.1.2 2021 yılının sonuna kadar personelimizi http://etwinningonline.eba.gov.tr/ da eğitimleri almasını sağlamak

Çevrim İçi Güvenlik Stratejisini Yürütme

2.4. Hareket Planı

Amaç	Activite	Sorumlu Kişi	Zaman Dilimi	Beklenen Sonuç/Girdi	Araçlar
Amaç 1.1.1 2021 yılında velilerimizin sosyal medya ile ilgili riskler konusunda okul farkındalığının artırılması.	<i>Seminerler vermek</i>	<i>Elçin İlaslan</i>	<i>Ocak 2021</i>	<i>1 saat içinde velilere sosyal medya ile riskler konusunda bilgilendirme</i>	<i>Bilgisayar Projeksiyon</i> https://www.guvenliweb.org.tr/
	<i>Broşurler vermek</i>	Helin Çelik	Şubat 2021	9 Şubat.2021 güvenli internet gününde sosyal medya ile ilgili riskler bilgilendirme	https://www.guvenliweb.org.tr/
Amaç 1.1.2 2021 yılında öğrencilerimizin sosyal medya ile ilgili riskler konusunda okul farkındalığının artırılması.	<i>Seminerler vermek</i>	<i>Elçin İlaslan</i>	<i>Ocak 2021</i>	<i>1 saat içinde öğrencilere sosyal medya ile riskler konusunda bilgilendirme</i>	<i>Bilgisayar Projeksiyon</i> https://www.guvenliweb.org.tr/
	<i>Broşurler vermek, panolar hazırlamak</i>	Sınıf Öğretmenleri	Şubat 2021	9 Şubat.2021 güvenli internet gününde sosyal medya ile ilgili riskler bilgilendirme	https://www.guvenliweb.org.tr/



<p>Amaç 1.1.3</p> <p>2021 yılında personelimizin sosyal medya ile ilgili riskler konusunda okul farkındalığının artırılması .</p>	Seminerler vermek	Elçin İlaslan	Şubat 2021	1 saat içinde personellerimize sosyal medya ile riskler konusunda bilgilendirme	Bilgisayar Projeksiyon https://www.guvenliweb.org.tr/
<p>Amaç 1.2.1</p> <p>2021 yılında velilerimize sınıf öğretmenleri tarafından e güvenlik konusunda bilgilendirme yapma</p>	Seminerler vermek	Elçin İlaslan	Şubat 2021	1 saat içinde e güvenlik konusunda bilgilendirme	Bilgisayar Projeksiyon https://www.guvenliweb.org.tr/
<p>Amaç 1.2.2</p> <p>2021 yılında öğrencilerimizin e güvenlik konusunda okul farkındalığının artırılması.</p>	Broşürler vermek,	Helin Çelik	Şubat 2021	9 Şubat.2021 güvenli internet gününde sosyal medya ile ilgili riskler bilgilendirme	https://www.guvenliweb.org.tr/
<p>Amaç 1.2.3</p> <p>2021 yılının sonuna kadar personelimizin e güvenlik konusunda okul farkındalığının artırılması.</p>	Seminerler vermek	Sınıf öğretmenleri	Şubat 2021	1 saat içinde e güvenlik konusunda bilgilendirme	Bilgisayar Projeksiyon https://www.guvenliweb.org.tr/
<p>Amaç 1.2.3</p> <p>2021 yılının sonuna kadar personelimizin e güvenlik konusunda okul farkındalığının artırılması.</p>	Pano hazırlamak	Sınıf Öğretmenleri	Şubat 2021	9 Şubat.2021 güvenli internet gününde pano hazırlama	Güvenli internet günü ile ilgili afişler ve resimler
<p>Amaç 1.2.3</p> <p>2021 yılının sonuna kadar personelimizin e güvenlik konusunda okul farkındalığının artırılması.</p>	Seminer vermek	Elçin İlaslan	Ocak 2021	1 saat içinde e güvenlik konusunda bilgilendirme	Bilgisayar Projeksiyon https://www.guvenliweb.org.tr/
<p>Amaç 1.3.1</p> <p>2021 yılında öğrencilerimizin siber zorbalığa ve cinsel içerikli mesajlara karşı korunması ve strateji geliştirmesinin artırılması.</p>	https://www.esafetylabel.eu/home	Kendisi	Yıl içinde	https://www.esafetylabel.eu/home üye olarak e güvenlik hakkında güncel verileri takip etmek	Bilgisayar
<p>Amaç 1.3.1</p> <p>2021 yılında öğrencilerimizin siber zorbalığa ve cinsel içerikli mesajlara karşı korunması ve strateji geliştirmesinin artırılması.</p>	Seminer	Sınıf öğretmeni	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>2021 yılında velilerimizin siber zorbalığa ve cinsel içerikli mesajlara karşı</p>	Müfredatın içinde işlemek	Sınıf öğretmeni	Yıl içinde	Yıl içinde derslerde bu konu ile ilgili bilgilendirme, drama yapma	Web siteleri
<p>Amaç 1.3.2</p> <p>2021 yılında velilerimizin siber zorbalığa ve cinsel içerikli mesajlara karşı</p>	Seminer vermek	Sınıf öğretmeni	Yıl içinde	Yıl içinde veli toplantılarında bu konu ile ilgili bilgilendirme yapma	Web siteleri



<p>korunması ve strateji geliştirmesinin artırılması.</p> <p>Amaç 1.3.3</p> <p>2021 yılında personellerimizin siber zorbalığa ve cinsel içerikli mesajlara karşı korunması ve strateji geliştirmesini arttırılması için seminerler vermek.</p>	Seminer vermek	Elçin İlaslan	Ocak 2021	1 saat içinde siber zorbalığa ve cinsel içerikli mesajlara karşı korunması konusunda bilgilendirme	Bilgisayar Projeksiyon https://www.guvenliweb.org.tr/
<p>Amaç 2.1.1</p> <p>2021 yılında personelimizin https://www.esafetylebel.eu/home a üye olmasını sağlamak</p>	Öğretmenler kurul toplantısı	kendisi	Yıl içinde	Yıl içerisinde https://www.esafetylebel.eu/home a üye olması ve blogları takip etmesini sağlamak	https://www.esafetylebel.eu/home
<p>Amaç 2.1.3</p> <p>2021 yılında personelimizin http://etwinningonline.eba.gov.tr/ da eğitimleri almasını sağlamak</p>	Öğretmenler Kurul toplantısı	Kendisi	Nisan 2021	Nisan ayındaki yapılacak olan ara tatilde kursları almak.	http://etwinningonline.eba.gov.tr/ “İnternet Güvenliği ve e Twinnin Etiği” ile “eSafety Label Hakkında Herşey” eğitimleri

3. İlerlemeyi İzleme ve Çevrim içi Güvenlik Stratejisini Değerlendirme

Odak Noktası	Stratejik Amaç	İlerleme Yada Amaç Nasıl Değerlendirilecek?	Zaman Aralığı
<p>Odak Noktası1</p> <p>Güvenli internet</p>	1.1 Sosyal medya ile ilgili riskler konusunda okul farkındalığının 1 yıl içinde %10 a çıkarmak.	Anketler yapılması ve web.güvenlik komisyonu tarafından belgelendirilmesi	Zaman1: Ocak 2021 Zaman2: Haziran 2021
	1.2 e-güvenliğin öneminin okul farkındalığını 1 yıl içinde %10 a çıkarmak	Anketler yapılması ve web güvenlik komisyonu tarafından belgelendirilmesi	Survey 1: Ocak 2021 Survey 2: Haziran 2021
	1.3 Öğrencilerin siber zorbalığa ve cinsel içerikli mesajlara karşı korunması ve strateji	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 2021 Survey 2: Haziran 2021

	geliştirmesini %10 a çıkarmak		
Personel	2.1 Personelin kendi güvenliği hakkında bilgilendirilmesini bir yılda %10 a çıkarmak.	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 2021 Zaman2:Haziran2021

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 veliyi bu konu hakkında bilgilendirmesi ve nasıl önlemler alabileceği hakkında görüşme yapılması - Öğretmenin web güvenlik komisyonuna bildirmesi. - Siber suçlar birimine 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. Okul internet ağı kullanıcı şifresinin öğrenciler tarafından keşfedilmesi	<ul style="list-style-type: none"> - Velilerimize uygun bir dille bunun yanlış olduğunu anlatılır. - Uzun şifrelerin belirlenmesi - Şifrelerde büyük küçük harf, sayı ve noktalama işaretlerin kullanılarak zorluk seviyesini arttırmak - Şifrelerin 3 ayda bir değiştirilmesi

WEB GÜVENLİK KOMİSYONU

Okul Müdürü	Kasım KONAK
Müdür Yardımcısı	Hatice KÖŞECİ
Rehber Öğretmen	Elçin İLASLAN
Sınıf Öğretmeni	Helin ÇELİK
Sınıf Öğretmeni	Şeniz AŞIK KILIÇOĞLU
İngilizce Öğretmeni	Nihan GÜRKEN

EKLER:**Lüleburgaz Atatürk İlkokulu Birincil Kabul Edilebilir Kullanım Politikası (AUP)**

- Lüleburgaz Atatürk İlkokulu ağını kullanarak, kullanım politikasını kabul etmiş olursunuz.
 - Bu kurallar okuldaki tüm bilgisayarların kullanımı için geçerlidir
 - İlkokul düzeyinde, öğrenciler internete yalnızca bir öğretmenin veya yetkili bir yetişkinin gözetimi altında erişebilir.
 - Filtreleme programı, okul ağını kullanan tüm elektronik cihazlara yüklenir.
 - Aşağıdakilerin tümünü kabul ediyorum.
- 1) Okuldaki bilgisayarları sadece okul çalışması için kullanacağım. Okulla ilgili olmayan materyalleri bilgisayarlara yüklemeyeceğim.
 - 2) İnterneti sadece öğretmenimin izni ile kullanacağım.
 - 3) Parolamı kimseye vermeyeceğim, başkalarının parolalarını istemeyeceğim.
 - 4) Kendime ve başkalarına resim veya bağlantı yüklemeyeceğim.
 - 5) Öğretmenimin onaylamadığı oyunları oynamayacağım.
 - 6) Bilgisayarda hem kendi adresim hem de telefon numaram; arkadaşlarımdan telefonlarını ve adreslerini yazmayacağım.
 - 7) Bilgisayar kullanırken düşünceli ve kibar olacağım. Başkalarını gücendirmek, sinirlendirmek, korkutmak, tehdit etmek, alay etmek ve zorbalık yapmak için kullanmayacağım. Küfür kullanmayacağım.
 - 8) Hiç kimsenin ırkı, dini ve cinsiyeti hakkında kötü ipuçları içeren materyalleri yüklemeyeceğim veya göndermeyeceğim.
 - 9) Başkasının işine zarar vermeyeceğim.
 - 10) Bir sorunla karşılaşırsam - siber zorbalık, cinsel mesajlaşma, uygunsuz içerik vb. - bunu kendim çözmeye çalışmayacağım. Öğretmenime söyleyeceğim. Okul öğretmenlerim ve yöneticilerim bu durumu hızla çözecekler.
 - 11) Okul bilgi sistemini engellemeye çalışmayacağım.
 - 12) Öğretmenim yaptığım işe bakıp kurallara uyup uymadığımı görebilir, kurallara uymazsam bir süre bilgisayar kullanmama izin verilmemesi gibi sonuçlarla karşılaşacağım.
 - 13) Okulda ailem veya diğer akrabalarım ile iletişime geçmem gerekirse, öğretmenim bunu sağlayacaktır.
- Öğrenci Adı Soyadı: _____ Sınıf: _____
Öğrenci İmzası: _____ Tarih: _____
- Ebeveynler: Kabul edilebilir kullanım politikasını çocuğumla okudum ve tartıştım ve bu koşullar altında bu kaynakları kullanmasına izin veriyorum.
- Ebeveynin Adı Soyadı: _____ Tarih: _____
Ebeveynin İmzası: _____
- * Öğrenciler bu sözleşmeyi imzalamadan ve öğretmenlerine götürmeden okuldaki bilgisayarları kullanamazlar.

Lüleburgaz Atatürk Primary School Acceptable Use Policy (AUP)

- By using the Lüleburgaz Atatürk Primary School network, you agree to the usage policy.
 - These rules are for the use of all computers in the school
 - At primary school, students have access to the Internet only under the supervision of a teacher or an authorized adult.
 - The filtering program is installed on all electronic devices using the school network.
 - I accept all of the below.
- 1) I will use the computers in the school only for school work. I will not upload school-unrelated material to computers.
 - 2) I will use the internet only with the permission of my teacher.
 - 3) I will not give my password to anyone, I will not ask for the passwords of others.
 - 4) I will not upload pictures or link to myself and others.
 - 5) I will not play games that my teacher does not approve of.
 - 6) I will not write neither my own address and phone number nor my friends' phones and addresses.
 - 7) I will be thoughtful and polite while using a computer. I will not use it to offend, annoy, scare, threaten, mock and bully others. I will not use swear language.
 - 8) I will not upload or send materials containing bad hints about anyone's race, religion, and gender.
 - 9) I will not harm anyone else's work.
 - 10) If I encounter a problem - cyberbullying, sexual messaging, inappropriate content, etc. - I will not try to fix it myself; I will tell my teacher. My school teachers and administrators will quickly resolve this situation.
 - 11) I will not try to prevent the school information system.
 - 12) My teacher can look at the work I do to see if I follow the rules, if I don't follow the rules, I will encounter results such as not being allowed to use a computer for a while.
 - 13) If I need to contact my family or other relatives at school, they will allow us to meet on my own phone or school phone if my teacher needs it.

Student Name Surname:

Class:

Student Signature:

Date:

Parents: I have read and discussed the acceptable use policy with my child, and I allow it to use these resources under these circumstances.

Parent's Name Surname:

Parent's Signature:

Date:

* Students cannot use the computers in the school without signing this contract and bringing it to their teacher.

LÜLEBURGAZ ATATÜRK İLKOKULU STRATEJİK eGÜVENLİK KURALLARI

Okulumuzda online güvenlik hizmeti geliştirilerek öğrencilerimizi, velilerimizi ve personelimizi bilinen her türlü tehditten korumak, bunlara karşı tedbirler almak ve yaşadıkları sorunları çözmek için stratejiler geliştirmek amaçlanmaktadır.

Öğretmenler, okul web sitesi, resim ve video paylaşımı, kullanıcılar, içerik, internet ve bilgi teknolojisi cihazlarının, cep telefonlarının ve kişisel teknoloji cihazlarının kullanımı ile ilgili kurallar belirlenmiştir.

a. Öğretmenler için:

1. Güvenlik politikalarının geliştirilmesi için yapılan toplantılara katkıda bulunmak,
2. Güvenlik için sorumluluk almak,
3. Teknolojiyi güvenle kullanmak,
4. Olası zararlı durumları gözlemlemek ve derhal önlem almak ve ilgili birime yönlendirmek,
5. <https://www.esafetylabel.eu/home> sitesindeki blogları ve formları takip ederek olası güvenlik sorunları ve çözümleri hakkında bilgi sahibi olmak

b. İnternet sitesi:

1. Web sitesi bir adres, telefon, faks ve e-posta adresi içerir.
2. Okul web yayın komisyonu tarafından onaylanan görüntüler yayınlanır.
3. Öğrencilerin çalışmaları velilerin izni ile yayınlanır.

c. Kullanıcılar:

1. Öğrenciler video hazırlamadan önce öğretmenlerinden izin almalıdır.
2. Görüntüden önce velilerden izin alınmalıdır.
3. Videolar ve konferanslar, resmi ve onaylı siteler aracılığıyla yapılmalıdır.
4. Kişisel sosyal medya hesaplarında, okul web yayın komisyonunun izni olmadan okul öğrencilerini ve çalışanlarını içeren görseller yayınlanamaz.
5. Öğrenciler Kabul Edilebilir Kullanım Politikasına uymalıdır.
6. Öğrencilere siber zorbalık veya cinsel mesajlarla karşılaştıklarında tavsiyelere, desteğe nasıl erişecekleri ve kendilerini nasıl koruyacakları öğretilir.
7. Öğrencilere kendilerini ve arkadaşlarını siber zorbalıktan, zararlı içeriklerden ve cinsel mesajlardan korumaları öğretilir.
8. Ebeveynlerimiz çocuklarıyla siber zorbalık ve cinsel mesajlar hakkında konuşmaları konusunda bilgilendirilir.
9. Velilerimiz, öğrencilerimiz güvenlikle ilgili sorunlarla karşılaştıklarında öğretmenleri veya danışmanlarıyla konuşmaları konusunda bilgilendirilir.

D. İnternet ve güvenli bilgi işlem cihazlarının kullanımı:

1. İnternetin yaygın kullanımı nedeniyle, güvenli internet kullanımı ve siber zorbalık konuları müfredata dahil edilmelidir.
2. Öğrenci ve öğretmenlerin en doğru bilgiye en güvenli şekilde ulaşmaları sağlanmalıdır.
3. İnternet erişimi öğrencilerin yaşlarına ve yeteneklerine göre sağlanır.
4. Uygun filtreleme yapılır ve güncellenir.
5. Paydaşlarımız yenilikler hakkında bilgilendirilir.
6. 09 Şubat 2021 "Güvenli İnternet Günü" okulumuzda kutlanacaktır.
7. Ağ güvenliği süreçleri cep telefonlarına ve kişisel cihazlara uygulanır.
1. Öğrencilerin okul saatleri içinde cep telefonu kullanmaları yasaktır.
2. Okulda veya bahçede izinsiz görüntülere, toplu fotoğraflara ve videolara izin verilmez.
3. Her öğrenci kendi kişisel cihazlarından sorumludur.

4. Yetkisiz erişimden kaynaklanan olumsuzlukların sorumluluğu kullanıcılara aittir.

5. Çalışanlar ders saatleri içinde telefonu sessize almak veya kapatmakla yükümlüdür.

Okulumuzda velilerimize, paydaşlarımıza güvenli internet konusunda seminerler verilmekte ve broşürler dağıtılmaktadır.

Siber zorbalık, cinsel içerikli mesajlaşma ve çocuk istismarı hakkında seminerlerle öğrencilere temel bilgiler sağlanır.

Web Okulumuzda bir web güvenlik komisyonu oluşturulmuştur.

Öğretmenlerimiz, <https://www.esafetylabel.eu/home>'a üye olmaya başladılar ve yenilikleri, gelişmeleri, blogları ve kaynakları takip etmeye çalışıyorlar. Bunun dışında, <http://etwinningonline.eba.gov.tr/> web sitesinde "İnternet Güvenliği" ve "E-Güvenlik Etiketleri Hakkında Her Şey" eğitimlerini alarak güncel bilgileri takip etme konusunda yönlendiriliyorlar.

E-güvenlik sorunları ile karşılaşan öğretmenler gerekli önlemleri alacak ve web güvenlik komisyonunu bilgilendirecektir.

LÜLEBURGAZ ATATÜRK PRIMARY SCHOOL STRATEGIC ESAFETY RULES

By developing online security service in our school, it is aimed to protect our students, parents and staff from all kinds of known threats, to take measures against them and to develop strategies to solve the problems they experience.

Rules for teachers, school website, image and video sharing, users, content, internet and the use of information technology devices, mobile phones and the use of personal technology device have been determined.

a. For Teachers:

1. Contributing to the meetings held to develop security policies,
2. Taking responsibility for security,
3. Using technology safely,
4. Observing potentially harmful situations and taking precautions immediately and directing them to the relevant unit,
5. To be informed about possible security issues and solutions by following blogs and forms on <https://www.esafetylevel.eu/home> site

b. Website:

1. The website contains an address, phone, fax and e-mail address.
2. The images approved by the school web publishing commission are published.
3. Students works are published with the permission of the parents.

c. Users:

1. Students must obtain permission from their teachers before preparing videos.
2. Permission must be obtained from parents before the image.
3. Videos and conferences should be done through official and approved sites.
4. In personal social media accounts, images containing school students and employees cannot be published without permission from the school web publishing commission.
5. Students must abide by the Acceptable Use Policy.
6. Students are taught how to access advice, support and protect themselves when they encounter cyber-bullying or sexual messages.
7. Students are taught to protect themselves and their friends from cyber-bullying, harmful content and sexual messages.
8. Our parents are informed to talk to their children about cyber-bullying and sexual messages.
9. Our parents are informed to speak to their teacher or counselor whenever our students encounter problems with security.

D. Use of Internet and secure computing devices:

1. Due to the widespread use of the Internet, the use of safe Internet and cyberbullying issues should be included to the curriculum.
2. It should be ensured that students and teachers access the most accurate information in the safest way.
3. The Access of Internet is provided according to students' ages and abilities.
4. Appropriate filtering is done and updated.
5. Our stakeholders are informed about innovations.
6. 09TH February, Safe internet day 2021 will be used in our school.
7. The processes of Network security are applied to mobile phones and personal devices.
 1. Students are prohibited from using mobile phones during school hours.
 2. Images, collective photos and videos are not allowed in the school or in the garden without permission.

3. Every student is responsible for his/her own personal devices.
4. Responsibility of the negativity arising from unauthorized access belongs to the users.
5. Employees are obliged to mute or hang up the phones during class hours.

Parents at our school, our stakeholders are given seminars about secure internet and the brochures are distributed.

Essential information is *provided for students* with seminars about cyber-bullying, and sexual content messaging and child abuse.

Web A web security commission has been established in our school.

Our teachers have started to become a member of <https://www.esafetylabel.eu/home> and are trying to keep up with innovations, developments, blogs and resources. Apart from this, they are guided to follow up-to-date information by taking "Internet Security" and "Everything About E-Security Label" trainings at <http://etwinningonline.eba.gov.tr/>

Teachers who encounter e-security problems will take the necessary measures and inform the web security commission.