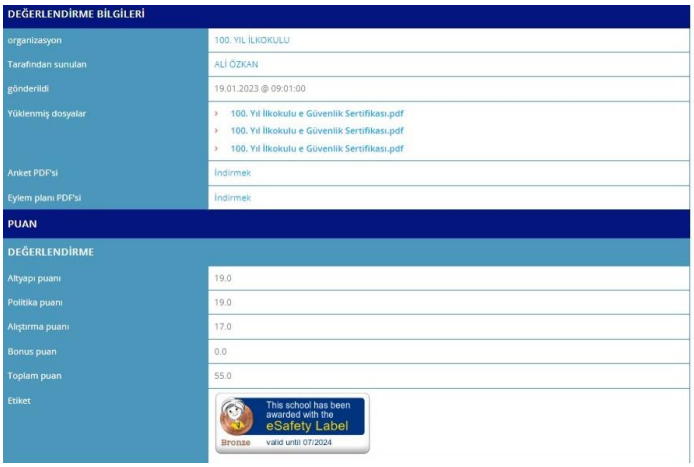
100. YIL İLKOKULU

e-Güvenlik Politikası 2022 - 2023

Amaç ve Kapsam

*(Bu politika **100. YIL İLKOKULU** içerisinde bulunan ağ erişimi bulunan her türlü teknolojik aleti ve kolej içerisinde bulunan yönetici, öğretmen, destek personeli, çocuk ve ebeveynler için hazırlanmış olup, sorumlulukları ve yaptırımları tüm herkesi kapsar. Okulumuz esafety label bronz etiket sahibi bir okuldur.)*



DEĞERLENDİRME BİLGİLERİ	
organizasyon	100. YIL İLKOKULU
Tarafından sunulan	ALİ ÖZKAN
gönderildi	19.01.2023 @ 09:01:00
Yüklenmiş dosyalar	100. Yıl İlkokulu e Güvenlik Sertifikası.pdf 100. Yıl İlkokulu e Güvenlik Sertifikası.pdf 100. Yıl İlkokulu e Güvenlik Sertifikası.pdf
Anket PDF'si	İndirmek
Eylem planı PDF'si	İndirmek
PUAN	
DEĞERLENDİRME	
Altyapı puanı	19.0
Politika puanı	19.0
Alıştırma puanı	17.0
Bonus puan	0.0
Toplam puan	55.0
Etiket	This school has been awarded with the eSafety Label Bronze valid until 07/2024

Dijitalleşen dünya, teknoloji ile sosyalleşmenin küçük yaşlara kadar inmesi ve eğitimde teknolojinin konumu gereği **100. YIL İLKOKULU** e-Güvenlik politikası;

- Eğitim standartlarını yükseltme,

- Öğrenci, veli, öğretmenleri ve diğer çalışanları e Güvenlik kapsamında koruma,

- 21 yüzyıl bilgi ve becerilerini güven içerisinde geliştirmeyi amaçlar.

Sorumluluklar

Çalışan Sorumlulukları

Okul e Güvenlik politikalarını okumak ve bağlı kalmak.

Öğrenci, veli, öğretmen ve diğer personel verilerini, şifre, bulut vb. yöntemlerle korumak.

Güncel teknoloji ve veri bilimleri konusunda bilgi sahibi olmak.

Dijital olarak saklanan kişiye ait verileri herkese açık ortamlarda paylaşmamak.

Kurum içerisinde resmi izin alınmadan öğrenci veya veli ile çekilen fotoğrafları medya hesaplarında paylaşmamak.

Öğrencinin kişisel telefonlarındaki bilgi ve verilere erişmeye çalışmamak.

Öğrencinin kişisel mesaj, fotoğraf ve tarayıcı geçmişlerine erişmeye çalışmamak.

Okul içerisinde kişisel cihazlardan ses kaydı ve video kayıtları özelliklerini etkinlik ve ders harici kullanmamak.

Okul içerisinde kişisel cihazlarından ders amacıyla kayıt ve video kullanımı gerekiyorsa, bilgilendirme konuşması ardından kayıt durumuna geçmek. Gizli ses kaydı ve video ders amacıyla dahi olsa kullanmamak.

Okul içerisinde kayıp DVD, CD, USB, disk vb. veri kayıt cihazlarını içeriğine bakmadan IT odasına teslim etmek.

Kişisel olarak zimmetlenmiş veya ortak kullanıma açık bilgisayarlar harici cihazları kullanmamak.

Okulda bulunan cihazlarda sosyal medya, mail, e Okul, e Devlet vb. kişisel kullanıcı adı ve şifre gerektiren hiç bir platformda hesaplarını açık bırakmamak. Tarayıcı deposunda “Beni Hatırla” butonunu işaretlememek.

Okulda bulunan veya okul tarafından zimmetlenmiş cihazları öğrencilerle, velilerle, yabancılarla paylaşmamak.

Okulda bulunan veya okul tarafından zimmetlenmiş cihazların arızalanması durumunda okul IT odasına teslim etmek. Arızalanan cihazı, farklı şirket/kuruma tamir ettirme amacıyla bırakmamak.

Okulda bulunan veya okul tarafından zimmetlenmiş cihazlara korsan/lisanssız yazılımlar kurmamak. Lisanslı yazılımları ise güncel versiyonda kullanmak.

Sorumlu olarak belleklere arşivlediği verileri, fiziksel kilitli dolaplarında tutmak.

Sorumlu olarak bulut sürücülerde arşivlediği verileri, güçlü bir şifre oluşturup, kimseyle paylaşmadan saklamak.

Öğrenci Sorumlulukları

Okul e Güvenlik politikalarını okumak ve bağlı kalmak.

Okulda kullandığı kişisel cihazlarını, okul girişinde bulunan öğrenci telefon kutusuna şifreli olarak kapalı bir biçimde bırakmak.

Okulda kullandığı, herkesin kullanımına açık cihazlarda, medya, bulut, mail vb. kişisel şifre ile koruduğu hesapları açık bırakmamak.

Laboratuvar ve sınıf içerisinde kendisine okul tarafından zimmetlenmiş bilgisayar, tablet vb. cihazlar dışında farklı kimselere zimmetlenmiş cihazları izinsiz kullanmamak.

Güvenlik kameralarının okulda bulunma amacını öğrenmek.

Okula dijital ortamda göndermesi gereken belgeleri, sadece okulun k12.tr uzantılı resmi adresine ya da k12.net uygulaması göndermek.

Okulda, kişisel cihazlarından etkinliklerde izin alma harici, görüntü ve ses kaydı almamak.

Öğrenci, öğretmen ve diğer personele ait kişisel cihazların verilerine erişmeye çalışmamak.

Okul içerisinde kayıp DVD, CD, USB, disk vb. veri kayıt cihazlarını içeriğine bakmadan IT odasına teslim etmek.

Öğrenci, öğretmen, veli ve diğer personele şantaj, zorbalık, tehdit içeren mesajlar göndermemek.

Öğrenci, öğretmen, veli ve diğer personelden aldığı şantaj, zorbalık, tehdit mesajları var ise aşağıda bulunan “Siber Zorbalık Sonrası Yol Haritası“ başlığı altında bulunan yol haritasını izlemek.

Okulda bulunan veya okul tarafından zimmetlenmiş cihazların arızalanması durumunda okul IT odasına teslim etmek. Arızalanan cihazı, farklı şirket/kuruma tamir ettirme amacıyla bırakmamak.

Okulda bulunan veya okul tarafından zimmetlenmiş cihazlara korsan/lisanssız yazılımlar kurmamak. Lisanslı yazılımları ise güncel versiyonda kullanmak.

Okul içerisinde kayıp DVD, CD, USB, disk vb. veri kayıt cihazlarını içeriğine bakmadan IT odasına teslim etmek.

Ebeveyn Sorumlulukları

Okul e Güvenlik politikalarını okumak ve bağlı kalmak.

Güvenlik Problemleri ve Siber Zorbalık ile mücadelede okul ile iş birliği içerisinde olmak.

Okul ağına bağlı iken kişisel mail, kişisel mesaj, banka işlemleri ve hukuken uygun olmayan eylemlerde bulunmamak.

Okul tarafından oluşturulmuş öğrenci kontrol yazılımları ve öğrenci servis ulaşım kontrol uygulamasını veri gizliliğini sağlayacak şekilde kullanmak. Hesap bilgilerini başkalarıyla paylaşmamak.

Öğrenci, öğretmen, veli ve diğer personele şantaj, zorbalık, tehdit içeren mesajlar göndermemek.

Okul içerisinde ve dışarısında, okula bağlı kimseler tarafından yaşanılacak güvenlik sorunu ve siber zorbalık durumunda okul idaresini bilgilendirmek.Öğrenci, öğretmen, veli ve diğer personelden aldığı şantaj, zorbalık, tehdit mesajları var ise aşağıda bulunan “Siber Zorbalık Sonrası Yol Haritası“ başlığı altında bulunan yol haritasını izlemek.

Kampüs içerisinde kişisel cihazlardan, etkinlik harici görüntü ve ses kaydı almamak.

Okul tarafından istenilen dijital verileri sadece okula ait k12.tr uzantılı adreslere yada k12.net uygulamasından göndermek.

Güvenlik

Çevrimiçi İletişim

Okul içerisinde iletişim sadece kurumsal mailler üzerinden gerçekleşmektedir.

Fiziksel Yapı ve Planlananlar

Next Generation Firewall cihazımızı, teknolojinin sunduğu imkanlar dahilinde en güncel halde tutmak ve yenilemek.

Tespit sistemini(IDS) güncel halde tutmak.

Content Filtering sistemi ile olumsuz içerikli sitelerin takibi ve bunların okul ağı tarafından engellenmesi.

Kişisel Cihazların Okul İçerisinde Kullanımı

Öğrenciler tarafından, acil durumlarda iletişime geçilecek kişiler sekreterlik bölümünde veri gizliliğini koruyacak şekilde tutulmaktadır. Okulda bulunan öğrencilerin kişisel cihaz kullanımı yasak olmakla beraber, iletişim özgürlüğü asla kısıtlanmamaktadır. Öğrenci isteği üzerine iletişim hakkı sağlanmaktadır.

Öğretmen, ebeveyn ve personel tarafından kişisel cihaz kullanımı politikalar kapsamında sınırlı olmak kaydıyla uygundur.

Siber Zorbalık

Siber zorbalık, bilgi ve iletişim teknolojilerini kullanarak bir birey ya da gruba yapılan teknik ya da ilişkisel tarzda zarar verme davranışlarıdır. Okul politikaları gereği bu tür durumlara sebebiyet veren kişiler 5237 sayılı Türk Ceza Kanunu 10. Bölüm düzenlenen yaptırımlara maruz kalmasıyla birlikte, okul tarafından disiplin kurulunca verilecek ek yaptırımlar ile de karşılaşacaktır.

Eğitim

Her yıl güncellenen içerikle Zararlı yazılımlar ve korunma yolları hakkında bilgilendirmeler IT birimi ve Rehberlik birimi ortak çalışması ile planlanıp, okul ajanda sistemine eklenmesi gerekmektedir.

Her yıl güncellenen içerikle sosyal medya kullanımı ve veri gizliliği konusunda eğitimlerin verilmesi için IT birimi ve Rehberlik Birimi ortak çalışma yürütecektir. Öğrenci ve velilerin bilgilendirilmesi için gerekli çalışmalar planlanıp okul ajanda sistemine eklenmesi gerekmektedir.

Her yıl güncellenen içerikle dijital vatandaşlık konusunda öğrencilerin bilgilendirilmesi için Ağustos öğretmen seminer döneminde IT departmanı ve bölüm başkanları ile görüşmeler sağladıktan sonra yapılacak olan etkinliklerin okul ajanda sistemine eklenmesi gerekmektedir.

Her yıl güncellenen içerikle Siber zorbalık ile mücadele için her yıl Eylül ayında okulun rehberlik birimleriyle ortak çalışmaların yürütülmesi ve yıl içerisinde yapılacak olan planın okul ajanda sistemine eklenmesi gerekmektedir.

Eğitmen Eğitimleri

Mesleki gelişimde, e Güvenlik konulu programlara minimum her iki yılda bir katılım şartı aranır.

Ebeveyn Eğitimi

Ebeveynlere e Güvenlik ve Siber Zorbalık ile ilgili yapılan araştırma ve önerileri içeren kitapçıklar her yıl güncellenerek gönderilir.

Sınıf öğretmenleri tarafından velilere, “Güvenlik Problemi” ve “Siber Zorbalık” durumlarında izlenmesi gereken yol haritası gönderilir.

Ebeveynlere özel uzmanlar tarafından seminerler verilir.

Personel Eğitimi

IT bölümü tarafından her yıl güncellenerek düzenlenen eğitim seminerlerinde güncel dijital güvenlik eğitimlerini alır.

Uygundur

12/09.2022

Ali ÖZKAN

Okul Müdürü

ÖĞRETMENİN İMZA SİRKÜSÜ

ADI-SOYADI İMZA

2022-2023 EĞİTİM-ÖĞRETİM YILI
100. YIL İLKOKULU
OKUL e-GÜVENLİK ÖĞRETMENLER KURULU TOPLANTISI

TOPLANTI TARİHİ: 28.12.2022 Çarşamba

TOPLANTI SAATİ: 10.00

GÜNDEM MADDELERİ

1. Açılış ve yoklama yapılması
2. Gündem maddelerinin okunması,
3. eTwinning Çalışmaları – e-Güvenlik, (19.09.2022 tarihi itibariyle 2022-2023 Öğretiminde Yürütülen Projeler)
4. 100. YIL İLKOKULU e-Güvenlik politikasının okunması ve geliştirilmesi; Taşınabilir cihazların/ cep telefonlarının kullanımı ile ilgili okulumuz e-güvenlik politikası doğrultusunda aşağıdaki kararlar alınması
5. E-Güvenlik konularının müfredat konularında yer verilmesi; aşağıda verilen sınıf, ders ünite ve kazanımlarla e-Güvenlik konularının ilişkilendirilmesi, e-Güvenlik farkındalığının geliştirilmesi;
6. E-Güvenlik konusunda personel eğitimi;
7. Veli bilgilendirme seminer ve toplantıları;
8. Öğrenci bilgilendirme çalışmaları;
9. Esafety, Okul Web Sitesinde e-Güvenlik ile ilgili bölümlerin oluşturulması ve geliştirilmesi;
10. Dilekler ve kapanış

GÖRÜŞMELER:

1) 28.12.2022 Çarşamba günü **Okul Müdürü Ali ÖZKAN** başkanlığında yapılan toplantıda ilk olarak açılış ve yoklama yapıldı. Toplantıya katılım sağlandığı görüldü.

2) Gündem maddeleri okunarak toplantı amacı **Okul Müdürü Ali ÖZKAN** tarafından açıklandı.

3) e-Twinning projeleri hakkında kısa bir değerlendirme yapan **Okul Müdürü Ali ÖZKAN** eTwinning portalı hakkında önceki seminer döneminde yapılan sunumu hatırlattı. Yapılan projelerin meyvesini vermeye başladığını, okulumuza bu sene eTwinning Okul Etiket adaylığı verildiğini belirtti. Bunun okulumuz için çok kıymetli bir unvan olduğunu bu yüzden başvuru yapmak ve etiketi aldıktan sonra da sürekliliğini sağlamak gerektiğini belirtti. Gerek öğrencilerin gerek öğretmen arkadaşların kaliteli çalışmalarının mutlaka ödül aldığını bu ödüllerin de okulumuzu değerli kılarak birçok yönden geliştirebileceğini hatırlattı. Sadece eTwinning çalışmalarını gerçekleştirirken değil okul içinde birçok çalışmayı sağlıklı bir şekilde sürdürebilmek için okul e-Güvenlik planını geliştirmek gerektiğini, öğretmen ve öğrencilerin siber zorbalığa maruz kalmamaları için çeşitli tedbirler alınmasının şart olduğunu ifade etti. Bu tedbirlerin odak noktasının da Milli Eğitim Bakanlığının bu konuyla ilgili yazı ve talimatları olduğunu bu yüzden bakanlığın konuyla ilgili her açıklaması ve resmi yazısının çok iyi takip edilmesinin gerekliliği üzerinde durdu. Bunun ardından Milli Eğitim Bakanlığının 2017/12 Okullarda Sosyal Medyanın kullanımı Genelgesi ve çevrimiçi derslerle ilgili resmi yazıları kurula okundu.

4) Çeşitli İlköğretim kurumlarının e-güvenlik politikalarından örnek kararlar okundu. Okulumuzda zaten öğretmen, öğrenci ve personelin e-güvenliği konusunda çalışmalar yapıldığı **Okul Müdürü Ali ÖZKAN** tarafından belirtildi. Örneğin öğrencilerin cep telefonlarını bilinçsiz kullanmasını önlemek amacıyla okula cep telefonu getirmediklerini, getirdikleri takdirde eğitim-öğretim günü içinde kullandırılmadığını hatırlattı.

Okul Öncesi Öğretmeni Melek KUNT seminer döneminde internet güvenliği hakkında personel bilgilendirmesi yapıldığını, sınıf rehber öğretmenlerinden sınıflarına bilinçli internet kullanımı bilgilendirmesi yapmalarını sağladıklarını belirtti. Aynı zamanda 2023 yılı Şubat ayında Güvenli İnternet gününün kutlanmasının da farkındalık yaratacağını söyledi. **Sınıf Öğretmeni Ayhan KUNT**'de panolarda öğrencilerin güvenli internet çalışmalarına yer verilmesinin güzel olacağını ve önümüzdeki Güvenli İnternet gününde de her kat panosuna çalışmalar asılmasının etkileyici olacağını belirtti. Bu sene öğrenci gelemeyeceği ihtimaline karşın Milli Eğitim Bakanlığı bünyesindeki güvenli internet görsellerinin kullanılabileceğini söyledi.

5) Bu maddeyi kapsayan Güvenli İnternet Nedir?

e-Güvenlik, Öğrenci ve Siber Zorbalık konularında **Sınıf Öğretmeni Ozan Ercan DİLEK,** ORGM tarafından hazırlanan kılavuzlar hakkında öğretmenlerimizi bilgilendirdi. Konuyla ilgili dokümanlara nasıl ulaşabilecekleri okulumuz öğretmenleriyle paylaşıldı. Öğrencilerin kameralarını kapatmaları nedeniyle ders öğretmeni ile göz teması kuramaması dezavantaj dahi olsa, her iki tarafında sağlıklı çevrimiçi ders işleyebilmeleri için uzaktan eğitimi öğrenmeleri ve bu doğrultuda hareket etmeleri gerektiğini belirtti. Aynı zamanda siber zorbalığın disiplin suçu olduğu, bu nedenle yönetmelik değişikliği yapıldığı önemle vurgulandı.

6) **Okul Müdürü Ali ÖZKAN**, **Okul Öncesi Öğretmenimizin** verdiği bilgiler doğrultusunda, öğretmenlerimizin eSafety portalına üye olmalarını ve okul e-Güvenlik Politikamızı geliştirmemiz gerektiğini önemle vurguladı. Bu konuda "tüm okul olarak birlikte hareket edeceğiz ve kararların sürekliliğini sağlayacağız" dedi.

7) Toplantı sonunda tüm katılımcı öğretmenlere teşekkür etti. Tüm okul öğretmenleri de bu yararlı toplantı için okul idaresine teşekkür ettiler ve aynı temenni ve iyi dileklerle toplantıya son verildi.

KARARLAR:

1) e-Güvenlik farkındalığının arttırılması için okul personeline, velilere ve öğrencilere eğitimler yapılmasına,

2) Taşınabilir cihazların/ cep telefonlarının kullanımı ile ilgili okulumuz e-güvenlik politikası doğrultusunda uyulması gereken kurallar güncellenmesine,

3) E-Güvenlik konularına, ders müfredatlarında yer verilmesine,

4) Şubat 2023 tarihinde Güvenli İnternet Günü'nün aktif bir şekilde kutlanmasına,

5) Okul Web Sitesinde e-Güvenlik ile ilgili bölümlerin oluşturulmasına ve geliştirilmesine,

6) Okulumuz e-Güvenlik Panosunun ve Güvenli İnternet Panosunun geliştirilmesine,

7) eTwinning proje ve çalışmalarında e-Güvenlik kurallarına uyulmasına,

8) Okulumuzun kendi çevrim içi güvenlik alt yapısını, politikalarını ve uygulamalarını ulusal ve uluslararası standartlara ulaştırmak ve e-güvenli okul olmak için eSafety çalışmalarının yürütülmesine karar verilmiştir.

Uygundur

28/12.2022

Ali ÖZKAN

Okul Müdürü

ÖĞRETMENİN İMZA SİRKÜSÜ

ADI-SOYADI İMZA

İŞİNİ ŞANSA BIRAKMA ÖNLEMİNİ AL

E-GÜVENLİK

UNUTMAYIN

E-GÜVENLİK

İnterneti güvenli ve bilinçli kullanmak için uymamız gereken kurallardır.Aynı zamanda diğer internet kullanıcılarıyla olan iletişimimizi de kapsar.

Peki Nasıl İnternette Güvende Kalabiliriz?

İnternette tanımadığın kişilere kişisel bilgilerini verme.Onların aslında kim olduğunu bilemezsin

Eğer internette birisi seni rahatsız ederse onu engellemekten çekinme

AÇIKLAMALAR:

1- HER SAYFA PARAFLANACAK, TOPLANTI TUTANAKLARI İMZALANACAK.
2- E GÜVENLİK PANOSU YAPILIP FOTOGRAFLANNARAK EKLENECEK.
3- BÜTÜN EVRAKLAR TARANIP BİRLEŞTİRİLEREK PDF ŞEKLİNDE YÜKLENECEK.
4- İMZASIZ OLARAK **e-Güvenlik Politikası 2022 – 2023 kısmı** WEB SİTEYE YÜKLENECEK. Okul sitesine sadece bu yüklenecek.
5- ESEP platformu başvuru yaparken **e-Güvenlik Politikası 2022 – 2023** imzalı, pdf şeklinde taranmış olarak yüklenecek.
6- Eklenilen resimler veya benzer resimler okul e güvenlik panosunda kullanılabilir.