




KAYRAK ŞEHİT UĞUR KATRAN İLKOKULU

e-Güvenlik Politikası 2022 - 2023



Amaç ve Kapsam

(Bu politika **Kayrak Şehit Uğur Katran İlkokulu** içerisinde bulunan ağ erişimi bulunan her türlü teknolojik aleti bulunan yönetici, öğretmen, destek personeli, çocuk ve ebeveynler için hazırlanmış olup, sorumlulukları ve yaptırımları tüm herkesi kapsar. Okulumuz e güvenliğe önem verir ve esafety label bronz etikete sahiptir.)

PUAN	
DEĞERLENDİRME	
Altyapı puanı	16.0
Politika puanı	20.0
Alıştırma puanı	20.0
Bonus puan	0.0
Toplam puan	56.0
Etiket	

Dijitalleşen dünya, teknoloji ile sosyalleşmenin küçük yaşlara kadar inmesi ve eğitimde teknolojinin konumu gereği **Kayrak Şehit Uğur Katran İlkokulu** e-Güvenlik politikası;

- Eğitim standartlarını yükseltme,
- Öğrenci, veli, öğretmenleri ve diğer çalışanları eGüvenlik kapsamında koruma,
 - 21 yüzyıl bilgi ve becerilerini güven içerisinde geliştirmeyi amaçlar.

Sorumluluklar

Çalışan Sorumlulukları

Okul eGüvenlik 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 setkinlik 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, eOkul, eDevlet 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 eGüvenlik 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 eGüvenlik 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 kişiler 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 gücün halde tutmak ve yenilemek.

Tespit sistemini(IDS) güncel halde tutmak.

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

SQL enjeksiyonları, parametre oynamaları, DDOS saldırıları, Çerez zehirlenmeleri ve siteler arası komut çalıştırma zaafiyetlerini (XXS) önleme yazılımlarını güncel tutma.

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 sağlandıktan sonra yapılacak olan etkinliklerin okul ajanda sistemine eklenmesi gerekmektedir.

Her yıl gncellenen ierikle Siber zorbalık ile mcadele iin her yıl Eyll ayında okulun rehberlik birimleriyle ortak alıřmaların yrtlmesi ve yıl ierisinde yapılacak olan planın okul ajanda sistemine eklenmesi gerekmektedir.

Her yıl T.C. Savunma Bakanlıęı ve T.C. Cumhurbaşkanlıęı Dijital Dnřm Ofisi tarafından Kasım ayının son haftası bařlatılan Siber Gvenlik Haftası evrimii etkinliklerine Fen ve Teknoloji Lisesi, Anadolu Lisesi ve ortaokul ęrencileriyle katılımın saęlanması planlanmaktadır.

Eęitmen Eęitimi

IT blm tarafından her yıl dzenlenen eęitim seminerlerinde gncel dijital gvenlik eęitimlerini alır.

Mesleki geliřimde, eGvenlik konulu programlara minimum her iki yılda bir katılım řartı aranır.

Ebeveyn Eęitimi

Ebeveynlere eGvenlik ve Siber Zorbalık ile ilgili yapılan arařtırma ve nerileri ieren kitapıklar her yıl gncellenerek gnderilir.

Sınıf ęretmenleri tarafından velilere, "Gvenlik Problemi" ve "Siber Zorbalık" durumlarında izlenmesi gereken yol haritası gnderilir.

Ebeveynlere zel uzmanlar tarafından seminerler verilir.

Personel Eęitimi

IT blm tarafından her yıl gncellenerek dzenlenen eęitim seminerlerinde gncel dijital gvenlik eęitimlerini alır.

PDR blm tarafından her yıl gncellenerek dzenlenen "siber zorbalık" seminerlerine katılım řartı aranır.



İŞİNİ ŞANSA BIRAKMA ÖNLEMİNİ AL

E-GÜVENLİK

UNUTMAYIN
GÜVENLİĞİNİZ SİZİN ELİNİZDE!

Çevrimiçi güvenliğini sağla





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

Eğer internette bir problemle karşılaşırsan bunu ailene veya öğretmenine söyle

