KAYNARCA ORTAOKULU
E-GÜVENLİK POLİTİKASI

Amaç ve Kapsam

(Bu politika Kaynarca Ortaokulu içerisinde bulunan ağ erişimi bulunan her türlü teknolojik aleti ve okul içerisinde bulunan yönetici, öğretmen, destek personeli, çocuk ve ebeveynler için hazırlanmış olup, sorumlulukları ve yaptırımları tüm herkesi kapsar.)

Dijitalleşen dünya, teknoloji ile sosyalleşmenin küçük yaşlara kadar inmesi ve eğitimde teknolojinin konumu gereği Kaynarca Ortaokulu 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 okul idaresine teslim etmek.
- ✓ Kişisel olarak zimmetlenmiş veya ortak kullanıma açık bilgisayarlar harici cihazları kullanmamak.
- ✓ Okulda bulunan cihazlarda sosyal medya, e-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 idaresine 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 sürümde 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.
- ✓ Okula kişisel cihazlarını getirmemek.
- ✓ Okulda kullandığı, herkesin kullanımına açık cihazlarda, medya, bulut, e-mail vb. kişisel şifre ile koruduğu hesapları açık bırakmamak.
- ✓ BT sınıfı 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 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 okul idaresine 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 idaresine 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 sürümde kullanmak.
- ✓ Okul içerisinde kayıp DVD, CD, USB, disk vb. veri kayıt cihazlarını içeriğine bakmadan okul idaresine 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 e-mail, kişisel mesaj, banka işlemleri ve hukuken uygun olmayan eylemlerde bulunmamak.
- ✓ 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.
- ✓ Okul içerisinde kişisel cihazlardan, etkinlik harici görüntü ve ses kaydı almamak.
- ✓ Okul tarafından istenilen dijital verileri sadece okula ait k12.tr uzantılı adreslere göndermek.

Güvenlik

Çevrimiçi İletişim

Okul içerisinde iletişim sadece kurumsal e-mailler üzerinden gerçekleşmektedir.

Fiziksel Yapı ve Planlananlar

Fatih Projesi kapsamında okulda bulunan cihazların bakımının sağlanması, arıza durumunda resmi yazışmaların yapılması sağlanmaktadır.

Kişisel Cihazların Okul İçerisinde Kullanımı

Öğrenciler tarafından, acil durumlarda iletişime geçilecek kişiler e-okulda tutulmaktadır. Okulda bulunan öğrencilerin kişisel cihaz kullanımı yasak olmakla beraber, iletişim özgürlüğü asla kısıtlanmamaktadır. Öğrenci isteği üzerine iletişim hakkı idare izni ile 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

Öğrenci Eğitimleri

Eğitim gören her öğrenci "Çevrimiçi Güvenlik" ve "Siber Zorbalık " alanlarında başta Bilişim Teknolojileri ve Yazılım dersinde, Sosyal Bilgiler dersinde ve Rehberlik servisi tarafından her yıl güncel eğitimlerini alır. Öğrenciler web uzantıları, bulut sistemi, fiziksel veri saklama cihazları, ağ sistemi konusunda eğitimler alır. Öğrencilere her yıl en az bir kere sanat, tasarım derslerinde "Çevrimiçi Güvenlik" ve "Siber Zorbalık" temalarında çalışmalar yaptırılarak bu konular hakkında bilinçlendirilmesi sağlanır.

Eğitmen Eğitimleri

MEB tarafından düzenlenen eğitim seminerlerinde güncel dijital güvenlik eğitimlerini alır. Mesleki gelişimde, e-Güvenlik konulu programlara sağlar.

Ebeveyn Eğitimi

Ebeveynlere e-Güvenlik ve Siber Zorbalık ile ilgili yapılan araştırma ve önerileri içeren broşürler gönderilir. Okul Rehber öğretmeni tarafından velilere, "Güvenlik Problemi" ve "Siber Zorbalık" durumlarında izlenmesi gereken yol haritası gönderilir.

Muharrem YÜRÜKOĞLU
Okul Müdürü