



EMİNE-AHMET YENİ KIZ ANADOLU İMAM HATİP LİSESİ

eGÜVENLİK OKUL POLİTİKASI

Bu politika metni, okulumuzun teknolojik gelişme ve yenilikler doğrultusunda günlük hayat ve eğitimde artan elektronik cihaz ve araçların kullanımı konusunda kurum bünyesinde yapılacak çalışmalar ve alınacak önlemler için bir çerçeve metnidir. Bu çalışmanın resmi dayanağı Milli Eğitim Bakanlığı Destek Hizmetleri Genel Müdürlüğü'nün 2018/10 nolu "Okullarda Güvenlik Önlemleri Alınması" konulu genelgesi ve bakanlık bünyesinde bulunan bilişim kaynaklarını kullanmasına yönelik usul ve esasların belirlendiği 11/04/2012 tarih ve 565 sayılı Bilgi ve Sistem Güvenliği Yönergesidir. Genelgenin ilgili alanları aşağıda alıntılanmıştır.

- y) Okul ve kurumlarda bilişim araçları ve sosyal medya kullanımında;
- 1) Zararlı, bölücü, yıkıcı, toplumun genel ahlak kurallarıyla bağdaşmayan ve şiddet içerikli amaçlar için kullanılmaması,
 - 2) Eğitim öğretim faaliyetlerine ve bireylere, maddi ve manevi zarar vermemeleri için gerekli tedbir ve gözetimlerin sürdürülmesi,
 - 3) Ahlak dışı ve şiddeti özendiren sesli, sözlü, yazılı ve görüntülü içeriklerin okul ve kurumlarda, eğitim ortamlarında izin verilmemesi,
 - 4) Derslik, laboratuvar vb. eğitim öğretim faaliyetlerinin yürütüldüğü alanlarda iletişim araçlarının kullanılmasına izin verilmemesi ve gerekli tedbirlerin alınması,

AMAÇ

Bilgi ve sistem güvenliği Yönergesine ulaşmak için [tıklayınız](#).

Okul yönetimi, öğretmenler, öğrenciler, yardımcı personel ve paydaşlarımıza yönelik yapılacak çalışmalar aşağıdaki amaçlar doğrultusunda planlanmıştır.

- Tüm Emine-Ahmet Yeni KAİHL ailesi üyelerini çevrimiçi olarak korumak ve güvenliğini sağlamak.
- Teknoloji kullanımından kaynaklanan potansiyel riskleri ve eğitimde teknoloji kullanımının yararları konusunda farkındalık yaratmak.
- Tüm personelin güvenli ve sorumlu bir şekilde çalışmasını sağlamak, olumlu davranışları etik kurallar çerçevesinde modellemek ve teknolojiyi kullanırken kendi standartlarını ve uygulamalarını yönetme ihtiyacının farkında olmak.
- Tüm paydaşlarımız tarafından bilinen çevrimiçi güvenlik endişelerine yanıt verirken açıkça kullanılacak prosedürleri tanımlamak.
- Yapılacak tüm eğitim-öğretim faaliyetleri, etkinlik ve projelerde çevrimiçi güvenlik konularında standartları belirlemek ve paydaşlarımızın çalışmalarını bu kurallar çerçevesinde yapmalarını sağlayarak eğitimin kalitesini artırmak.

Çalışan Sorumlulukları

- Okul eGüvenlik politikalarını okumak ve bağlı kalmak ve geliştirilmesine katkıda bulunmak.
- Güncel teknoloji ve veri güvenliği konusunda bilgi sahibi olmak. Milli Eğitim Bakanlığı Öğretmen Bilişim Ağında bulunan “Dijital Vatandaşlık Eğitimi Kursu” eğitimini almış olmak.
- Okul sistemlerinin ve verilerin güvenliği konusunda dikkatli ve bilinçli davranmak. Fiziksel güvenlik önlemleri ve şifre güvenliği konusunda kurallara uygun davranmak.
- Okul içi yapılan etkinlik, organizasyon ve elde edilen başarıların çevrimiçi duyurularında güvenlik ve mahremiyet konularında bilinçli ve duyarlı davranmak.
- eGüvenlik ile ilgili duyuru, seminer, bilgilendirme toplantısı gibi etkinlikleri takip etmek, bilgilerini güncellemek, farkında olmak. eGüvenlik konularını mümkün olduğunca müfredatla ilişkilendirip eğitim-öğretimin ayrılmaz bir parçası olarak görmek.
- Ortak kullanımda olan bilgisayar ve etkileşimli tahtalarda kişisel hesaplarının güvenliğini sağlamak, hesapları açık bırakmamak. Hesap açılacaksa “Beni Hatırla” seçeneğini devre dışı bırakmak, tarayıcıda verilerin saklanmasını engellemek.
- Ortak kullanımda olan elektronik cihazların (bilgisayar, etkileşimli tahta, yazıcı, harici donanım ve ekipmanların) arızalanması ya da amaca uygun hizmet vermemesi durumunda okul Bilişim Teknolojileri Rehberlik Servisine bildirimde bulunmak.
- Elektronik cihazların konumlarını varsa IP adreslerini, erişilebilirlik bilgilerini BTR Servisine bildirilmeden değiştirmemek.
- Okulda bulunan veya okul tarafından zimmetlenmiş cihazlara korsan/lisanssız yazılımlar kurmamak. Lisanslı yazılımları ise güncel versiyonda kullanmak.

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.
- 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.
- 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

- Çocuklarıyla çevrimiçi güvenlik konularını tartışmak, okulun çevrimiçi güvenlik yaklaşımlarını desteklemek ve evde uygun güvenli çevrimiçi davranışları pekiştirmek.

- Okul Kabul Edilebilir Kullanım Politikalarını okumak, çocuklarını bu politikaya bağlı kalmaya teşvik etmek ve uygun olduğunca kendilerinin de bağlı kalmasını sağlamak.
- Teknoloji ve sosyal medyanın güvenli ve uygun kullanımını modellemek.
- Davranışlarında, çocuğun çevrimiçi olarak zarar görme tehlikesi altında olduğunu gösteren değişiklikleri belirlemek.
- Okul veya diğer uygun kurumlardan, kendileri ve ya çocukları çevrimiçi problem veya sorunlarla karşılaşırsa yardım veya destek istemek.
- Okulun çevrimiçi güvenlik politikalarının oluşturulmasına katkıda bulunmak, güvenlik problemleri ve siber zorbalık ile mücadelede okul ile iş birliği içerisinde olmak.
- Okul tarafından oluşturulmuş öğrenci kontrol yazılımları ve öğrenci servis ulaşım kontrol uygulamasını veri gizliliğini sağlayacak şekilde kullanmak. Hesap bilgilerini başkalarıyla paylaşmamak.

Okulun Ağ Altyapısı ve İnternet Erişimi

- Ağ bağlantı cihazları tek bir merkezde bulunan ve yüklenici firma tarafından tasarımı yapılan ağ altyapısı ve sadece kablolu internet bağlantısı bulunan okulumuzda, tüm bilgisayar ve etkileşimli tahtalar aynı ağda bulunmaktadır.
- Etkileşimli tahtalarda her öğretmenin kendi USB anahtarı ve EBA'da tanımlı kullanıcı hesabı vardır, öğretmenlerin kişisel şifrelerini öğrencilerle paylaşmamaları gerekmektedir.
- Öğretmen hesapları dışında Etkileşimli tahtaların öğrenci hesapları öğrenci erişimine açıktır. Yönetici hesap şifresi ve tahtalarla ilgili tüm sorumluluk okulumuz BTR Öğretmenine aittir.
- 12. Ve 8. Sınıf öğrencilerimizin ders dışında da tahtaları eğitim amaçlı kullanımlarına izin verilir.
- İnternet erişim cihazımızın kablosuz ağ bağlantı özelliği bulunmaktadır, ancak kablosuz ağın ortak kullanımına izin verilmemektedir.
- Ağ bağlantı cihazlarının bulunduğu sistem odasına öğrenci girişine kapalıdır.
- İnternet servis sağlayıcı tarafından MEB tarifesi ile filtre uygulanan internet erişimimiz, kullanıcıların uygunsuz ve reklam içeriklerinden korunmasını sağlamaktadır.
- Kullanıcıların şahsi internet erişimlerini eğitim faaliyetlerinde kullanmaları istenmeyen bir durumdur.

Okul Web Sitesi ve Sosyal Medya Hesapları

- Okul web sitesi ve sosyal medya hesapları bir komisyon tarafından yönetilmektedir. Paylaşımların sorumluluğu okul müdürüne ait olup, içeriklerin tamamı onayı olmadan paylaşılmamaktadır.
- Paylaşımların etkileşim trafiği ve paylaşımlara yapılan yorumlar hesap yöneticileri tarafından kontrol edilmekte, istenmeyen etkileşimler engellenmektedir.
- Sosyal medya hesap bilgileri, iki aşamalı güvenlik önlemleri ile sağlanmış, yetkisiz kişilerle paylaşılmaması konusunda gerekli hassasiyet gösterilmektedir.
- Okulumuzun misyonu doğrultusunda tanıtımı, yapılan etkinlik ve organizasyonların yaygın etkisinin artırılması için özellikle sosyal medya hesapları etkin ve verimli şekilde kullanılmaktadır, özgün içeriklerle sürekli güncel tutulmaktadır.
- Tüm öğretmenlerimizin yaptıkları etkinlik, organizasyon ve başarılarına ait paylaşımlarla ilgili görsel materyallerin öğrenci ve kurum veri mahremiyetine uygun şekilde teslim etmelidir.
- Görüntü politikasına uygun olarak, öğrencilerin resimlerinin / videolarının elektronik olarak yayınlanmasından önce her zaman ebeveynlerin yazılı izni alınacaktır.

- Tüm çalışanlar ve öğrenciler eğitim-öğretim yılının başında çevrimiçi güvenlik ve alınması gereken önlemler konusunda bilgilendirilir. Yıl içerisinde “Güvenli İnternet Günü” ve “Siber Güvenlik Haftası” etkinlikleri kapsamında bilinçlendirme ve farkındalık çalışmaları devam eder.
- Öğrencilerimiz EBA üzerinden Siber Güvenlik Portalına yönlendirilir, zengin içerik ve oyunlarla farkındalıkları artırılır.
- Öğretmenlerimiz ÖBA üzerinden “ Dijital Yurttaşlık Eğitimi Kursu” almaya yönlendirilir. Müfredatlarına uygun şekilde derste bu konuları işlemeleri teşvik edilir.
- Bilgilendirme ve güncel duyurular için okul panosu hazırlanır. Pano hazırlanırken öğrenci işbirliğine önem verilir.
- Afiş ve broşür çalışması yapılarak konunun yıl boyunca gündemde olması sağlanır.
- Her yıl güncellenen içerikle zararlı yazılımlar ve korunma yolları hakkında bilgilendirmeler BT birimi ve Rehberlik birimi ortak çalışması okul etkinlik planına eklenmektedir.
- 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.
- Etkileşimli tahtalar ve bilişim teknolojileri sınıfında bulunan öğrenci bilgisayarlarında TÜBİTAK tarafından geliştirilen açık kaynak kodlu PARDUS işletim sistemi ve uyumlu uygulama yazılımları kullanılmaktadır. Bu yazılımların güvenlik konusunda sağladığı avantajlar ve kullanımları ile ilgili bilgilendirmeler yapılmaktadır.