



AYDIN MESLEKİ VE TEKNİK ANADOLU LİSESİ

e-güvenlik politikası

2022 – 2023

Bu politika okulun tüm üyeleri (personel, öğrenciler, gönüllüler, ebeveynler / çalışanlar, ziyaretçiler dahil) için geçerlidir, hem okul içinde hem de dışında okul BIT sistemlerine erişimi olan ve bunları kullanan topluluk kullanıcıları).

Okul Müdürlerine makul olduğu ölçüde aşağıdaki davranışları düzenleme yetkisi vermektedir öğrencilerin okul dışında buldukları zamanki durumları hakkında bilgi verir ve personele aşağıdaki durumlarda disiplin cezaları uygulama yetkisi verir. Bu, siber zorbalık olayları veya bu politika kapsamındaki diğer e-güvenlik olaylarıyla ilgilidir, Okul dışında da gerçekleşse de okul üyeliğiyle olduğu için bağlayıcılığı vardır.

İnternet ve çevrimiçi teknoloji gençlerin öğrenmesi ve gelişmesi için yeni fırsatlar sunmakla birlikte onları yeni tür risklere de maruz bırakabilir. E-güvenlik, okulların ve kolejlerin koruma ve çocuk koruma önlemlerinin temel bir parçasını oluşturmaktadır.

E-güvenlik söz konusu olduğunda üç önemli risk alanı içerik, temas ve davranışlardır. İçerik, çevrimiçi olarak erişilen materyalle ve bu materyalin zararlı, yasadışı ve/veya uygunsuz olup olmadığıyla ilgilidir. Bu metin, ses, görüntü veya video gibi çeşitli formatlarda olabilir.

E-güvenlik öğretimi, çocukların uygunsuz içerik, davranış, iletişim ve ticariliği tanımalarına yardımcı olmaya odaklanır ve uygun şekilde nasıl yanıt vereceklerini veya tepki göstereceklerini öğrenmelerine yardımcı olur. Öğrenciler çevrimiçi zorbalığın etkilerinin farkındadır ve bu sorunlardan etkilenmeleri halinde nasıl yardım isteyeceklerini bilirler.

Çevrimiçi ortamda güvende olmak, bireylerin kendilerini ve başkalarını, kişisel bilgilerini tehlikeye atabilecek, güvenli olmayan iletişimlere yol açabilecek ve hatta ruh sağlıklarını ve refahlarını etkileyebilecek çevrimiçi zararlardan ve risklerden korudukları anlamına gelir.

Okulda İnternet Güvenliđini nasıl teŖvik etmeliyiz

Öđrenciler için Akıllı Telefon İpuçları okulda duyurulacaktır:

1. Adresiniz, Ŗifreleriniz, telefon numaranız gibi kiŖisel bilgilerinizi asla paylaŖmayın.
2. Sadece tanıdıđınız kiŖileri ekleyin.
3. Ailenizin veya gelecekteki iŖverenlerinizin gormesini istemeyeceđiniz hiřbir Ŗeyi asla yayınlamayın.
4. Ekran zamanını yeŖil zaman ile dengeleyin.
5. Çevrimiçi ortamda kibar olun.
6. Okul saatlerinde telefonunuzu ulaŖılamayacak bir yerde tutun.

Okulumuzda Öđrencilerin Çevrimiçi Ortamda Güvende ve Emniyette Kalmalarına Yardımcı Olmanın Yolları Ŗu Ŗekildedir.

1. 9 Sınıfta Eđitimler BaŖlayacak.
2. Öđrencilere Dijital Okuryazarlık Öđretilecek.
3. Veri Madenciliđi Yapmaları için teŖvik edilecekler
4. Sosyal Medyada Gizlilik Ayarlarının Kontrol Edilmesini öđretilecek
5. Dijital Bakımın Önemini anlatılacak
6. Anlatmak İstediđinizi Kanıtlamak için Gerçek Dünya Senaryolarını kullanılacak

Müdür ve Müdür Yardımcıların Görevleri

- Müdür, okul üyelerinin güvenliđini (e-güvenlik dahil) sađlamakla yükümlüdür
- Müdür ve (en azından) Müdür Yardımcısı ve ilgili ekibin baŖkanı tüm bu konulardan haberdar olmalıdır. Bir üyeye karŖı ciddi bir e-güvenlik iddiasında bulunulması durumunda izlenecek prosedürler personel sayısını belirlemelidir
- Müdür ve Müdür Yardımcısı, E-Güvenlik Koordinatörünün ve diđer ilgili personelin e-güvenlik rollerini yerine getirebilmeleri için uygun eđitimi almalarını sađlamaktan ve ilgili diđer meslektaŖlarını eđitmekten sorumludur
- Müdür, okulda dahili e-güvenlik izleme rolünü yürütenlerin izlenmesine ve desteklenmesine olanak tanıyan bir sistemin mevcut olmasını sađlayacaktır. Okul için bir güvenlik ađı sađlamakla yükümlüdür.

Ağ Yöneticisi / Teknik personel

Dijital ve BT Direktörü aşağıdakileri sağlamaktan sorumludur:

- Okulun teknik altyapısının güvenli olması ve kötüye kullanıma veya kötü niyetli saldırılara açık olmaması
- Okulun gerekli e-güvenlik teknik gereksinimlerini ve KHDA / diğer ilgili kurumları karşılaması. Uygulanabilecek E-Güvenlik Politikası / Kılavuzun detaylarıyla hazırlanması
- Kullanıcıların ağlara ve cihazlara yalnızca uygun şekilde uygulanan bir parola ile erişebilmesi Şifrelerin düzenli olarak değiştirildiği koruma politikası
- Filtreleme politikası (eğer varsa) düzenli olarak uygulanır ve güncellenir ve uygulama tek bir kişinin sorumluluğunda olmamasını sağlamak
- E-güvenlik görevlerini etkin bir şekilde yerine getirebilmek için e-güvenlik teknik bilgilerini güncel tutma rolünü üstlenmek. İlgili diğer kişileri bilgilendirmek ve bilgilerini güncel tutmak
- Ağ / internet / Sanal Öğrenme Ortamı / uzaktan erişim / e-posta kullanımının düzenli olması Herhangi bir kötüye kullanımın / kötüye kullanım girişiminin Müdüre rapor edilebilmesi

Öğretmen ve Destek Personeli şunları sağlamaktan sorumludurlar

- E-güvenlik konularında ve mevcut okul / akademi e-güvenliği hakkında güncel bir farkındalığa sahip olmak
- Şüphelenilen herhangi bir kötüye kullanım veya sorunu soruşturma / eylem / yaptırım için müdürü bildirirler
- Öğrenciler / ebeveynler / çalışanlar ile tüm dijital iletişimler profesyonel düzeyde olmalı ve sadece resmi okul sistemleri kullanılarak gerçekleştirilmiştir
- E-güvenlik konuları müfredatın ve diğer faaliyetlerin tüm yönlerine işlemek
- Öğrenciler e-güvenlik ve kabul edilebilir kullanım politikalarını anlamak, bilmek
- Öğrenciler, araştırma becerileri ve intihalden kaçınma ve intihalden uzak durma gerekliliği konusunda bilgi sahibi olmak
- Derslerde ve diğer etkinliklerde dijital teknolojilerin, mobil cihazların, kameraların vb. kullanılmayacağını bilmek. Okul etkinlikleri (izin verilen yerlerde) ve bu cihazlarla ilgili mevcut politikaların uygulamak
- İnternet kullanımının önceden planlandığı derslerde öğrenciler, aşağıdakiler için uygun olduğu kontrol edilen sitelere yönlendirmek ve internette bulunan uygunsuz materyallerle başa çıkmak için süreçleri yürütmek.

Öğrenciler

- Okul dijital teknoloji sistemlerini Öğrenci Yönetmeliğine uygun olarak kullanmaktan sorumludurlar.
 - Araştırma becerileri ve intihalden kaçınma ve telif haklarını koruma ihtiyacı konusunda Bilgi sahibidir
 - İstismar, kötüye kullanım veya uygunsuz materyallere erişimi bildirmenin önemini anlamaları gerekir ve bunu nasıl yapacağını bilir
 - Mobil cihazların ve dijital kameraların kullanımına ilişkin politikaları bilmeleri ve anlamalandırmalarını bilir
- Ayrıca görüntülerin alınması/kullanılması ve siber zorbalıkla ilgili politikaları da bilmeli ve anlamalıdır.
- Dijital teknolojileri kullanırken iyi e-güvenlik uygulamalarını benimsemenin önemini anlamalıdır.
- Okul dışında ve okulun E-Güvenlik Politikasının okul dışındaki eylemlerini de kapsadığının farkında olur.

AYDIN MESLEKİ VE TEKNİK ANADOLU LİSESİ MÜDÜRLÜĞÜ