KIRIMLI FAZİLET OLCAY ANADOLU LİSESİ E GÜVENLİK POLİTİKAMIZ

ÇEVRİMİÇİ ORTAMDA VAR OLAN BAZI BİLİŞİM SUÇLARI

1. Bilgisayar Sistemlerine ve Servislerine Yetkisiz Erişim
2. Bilgisayar Sabotajı
3. Bilgisayar Yoluyla Dolandırıcılık
4. Bilgisayar Yoluyla Sahtecilik
5. Bir Bilgisayar Yazılımının İzinsiz Kullanımı
6. Kişisel Verilerin Kötüye Kullanılması
7. Sahte Kişilik Oluşturma ve Kişilik Taklidi
8. Yasadışı Yayınlar
9. Ticari Sırların Çalınması
10. Terörist Faaliyetler
11. Çocuk Pornografisi
12. Hacking
13. Diğer Suçlar (Organ, fuhuş, tehdit, uyuşturucu, vb.)

Güvenli İnternet kapsamında okulumuzda Öğretmenlere, Öğrencilere ve idarecilere sürekli aktarılan konular:

-Zayıf Parola Oluşturulmaması,

-Ortak internet kullanımında zararlı içerikli sitelere girmeye çalışılmaması,

-Şifrenin Öğrencilerle Paylaşılmaması,

-Kayıtlı cihazlar dışında başka bir cihazdan erişim sağlanmaması,

-Kurumumuzda Kişisel verilerimizin bilinçsizce toplanmaması,

-Küçük yaşta sosyal medya kullanılmasına özendirilmemesi,

-Bilinçsizce mobil uygulamaların yüklenmemesi,

-Sahte Hesaplara tıklanmamasına dikkat edilmesi

OKULUMUZDAKİ E-GÜVENLİK POLİTİKASININ AMACI

OKULUMUZDA, güvenli ve güvenli bir ortam olduğundan emin olmak için, toplumun tüm üyelerinden beklenen ana ilkeleri, güvenli ve sorumlu kullanım teknolojisi ile ilgili olarak tanımlamak.

OKULUMUZDA, tüm üyelerini çevrimiçi olarak korumak ve güvenliğini sağlamak.

Teknolojinin potansiyel riskleri ve yararları konusunda topluluğunun tüm üyelerinde farkındalık yaratmak.

Tüm personelin güvenli ve sorumlu bir şekilde çalışmasını sağlamak, olumlu davranışları online olarak modellemek ve teknolojiyi kullanırken kendi standartlarını ve uygulamalarını yönetme gereksiniminin farkında olmak.

Okuldaki tüm üyeler tarafından bilinen çevrimiçi güvenlik endişelerine yanıt verirken açıkça kullanılacak prosedürleri tanımlamak.

Bu politika, internet erişimi ve kişisel cihazlar da dahil olmak üzere bilgi iletişim cihazlarının kullanımı için geçerlidir; çocuklar, personel ya da diğer kişilere, çalıştıkları dizüstü bilgisayarlar, tabletler veya mobil cihazlar gibi uzaktan kullanım için okul tarafından verilen cihazlar için de geçerlidir.

TÜM ÇALIŞANLARIN KİLİT SORUMLULUKLARI ŞUNLARDIR

-Çevrimiçi güvenlik politikalarının geliştirilmesine katkıda bulunmak.

-Kabul Edilebilir Kullanım Politikalarını (AUP´lar) okumak ve onlara bağlı kalmak.

-Okul sistemlerinin ve verilerin güvenliğinden sorumlu olmak.

-Bir dizi farklı çevrimiçi güvenlik konusundaki farkındalığa sahip olmak ve onların bakımında çocuklarla nasıl ilişkili olabileceklerini bilmek.

-Yeni ve gelişmekte olan teknolojiler kullanıldığında iyi uygulamaları modelleme.

-Mümkün olduğunca müfredat ile çevrimiçi güvenlik eğitimini ilişkilendirme.

-Okul koruma politikalarını ve prosedürlerini takip ederek endişe duyan bireylerin belirlenmesi ve uygun önlem alınması.

-Kişisel ve kişisel teknoloji kullanımlarında, hem açık hem de kapalı alanda profesyonel bir davranış seviyesinin korunması.

-Olumlu öğrenme fırsatlarına vurgu yapmak.

-Bu alanda mesleki gelişim için kişisel sorumluluk almak.

1-Öğrencilerimizin başlıca sorumlulukları şunlardır:

-Çevrimiçi güvenlik politikalarının geliştirilmesine katkıda bulunmak.

-Okulun Kabul Edilebilir Kullanım Politikalarını (AUP´lar) okumak ve onlara bağlı kalmak.

-Çevrim içi ve çevrimdışı başkalarının hislerine ve haklarına saygı duymak.

-İşler ters giderse, güvenilir bir yetişkinden yardım istemek ve çevrimiçi güvenlik sorunlarıyla karşılaşan diğer kişileri desteklemek.

-Kendilerini ve başkalarını çevrimiçi olarak korumak için sorumluluk almak.

-Yeni ve gelişmekte olan teknolojilerin getirdiği fırsatlar ve risklerle ilgili olarak kendi bilinci ve öğrenimlerinden sorumlu olmak.

-Belli bir teknolojiyi kullanmanın kişisel risklerini değerlendirmek ve bu riskleri sınırlamak için güvenli ve sorumluluk sahibi davranmak.

2-Ebeveynlerin başlıca sorumlulukları şunlardır:

-Okul Kabul Edilebilir Kullanım Politikalarını okumak, çocuklarını bu politikaya bağlı kalmaya teşvik etmek ve uygun olduğunca kendilerinin de bağlı kalmasını sağlamak.

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

-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.

-Öğrenme platformları ve diğer ağ kaynakları gibi okul sistemlerini güvenli ve uygun bir şekilde kullanmak.

-Yeni ve gelişmekte olan teknolojilerin getirdiği fırsatlar ve risklerle ilgili olarak kendi bilinci ve öğrenimlerinden sorumlu olmak.

EVRİMİÇİ İLETİŞİM VE TEKNOLOJİNİN DAHA GÜVENLİ KULLANIMI

1-Okul / web sitesinin yönetilmesi

-Web sitesinde iletişim bilgileri okul adresi, e-posta ve telefon numarası olacaktır. Personel veya öğrencilerin kişisel bilgileri yayınlanmayacaktır.

-Okul Müdürü yayınlanan çevrimiçi içerik için genel yayın sorumluluğunu alacak ve bilgilerin doğru ve uygun olmasını sağlayacaktır.

-Web sitesi, erişilebilirlik fikri mülkiyet haklarına saygı, gizlilik politikaları ve telif hakkı da dahil olmak üzere okulun yayın yönergelerine uyacaktır.

-Spam maillerden korunmak için e-posta adresleri çevrimiçi olarak dikkatli bir şekilde yayınlanacaktır.

-Öğrenci çalışmaları öğrencilerin izniyle ya da ebeveynlerinin izniyle yayınlanacaktır. Her Dönem Başında tüm velilerden öğrencilerin resimleri, çalışmaları, eserleri, etkinliklerinin okulumuz Web Sitesi, eTwinning Projeleri, Eba Haber de yayınlanmasını uygun gördüğüne dair ''Veli İzin Beyanı'' alınacaktır.

-Okul web sitesinin yönetici hesabı, uygun bir şekilde güçlü şifreyle şifrelenerek korunacaktır.

2-Kullanıcılar

-Öğrenciler, bir video konferans araması veya mesajı hazırlamadan veya cevaplamadan önce bir öğretmenin izin isteyecektir.

-Video konferans, öğrencilerin yaşı ve yeteneği için uygun bir şekilde denetlenecek.

-Velilerin rızası, çocuklar video konferans faaliyetlerine katılmadan önce alınacaktır.

-Video konferans, sağlam bir risk değerlendirmesini takiben, resmi ve onaylanmış iletişim kanalları vasıtasıyla gerçekleşecektir

-Sadece ana yöneticilere video konferans yönetim alanlarına veya uzaktan kumanda sayfalarına erişim hakkı verilecektir.

-Eğitimsel video konferans servisleri için özel oturum açma ve şifre bilgileri yalnızca personellere verilecek ve gizli tutulacak.

3-İçerik

-Okulun internet erişimi eğitimi geliştirmek ve genişletmek için tasarlanacaktır.

-İnternet erişim seviyeleri müfredat gerekliliklerini ve öğrencilerin yaş ve yeteneklerini yansıtacak şekilde gözden geçirilecektir.

-Çalışanların tüm üyeleri, çocukları korumak için tek başına filtrelemeye güvenmeyeceklerinin farkındadır ve gözetim, sınıf yönetimi ve güvenli ve sorumlu kullanım eğitimi önemlidir.

-İçerik; Öğrencilerin yaşlarına ve yeteneklerine uygun olacaktır.

-Tüm okul ait cihazlar, okulun Kabul Edilebilir Kullanım Politikasına uygun olarak ve uygun güvenlik ve güvenlik önlemleri alınarak kullanılacaktır.

-Personel üyeleri, web sitelerini, araçlarını ve uygulamalarını sınıfta kullanmadan önce veya evde kullanmayı önerirken daima değerlendirecektir.

-Öğrenciler, bilginin konumlanması, alınması ve değerlendirilmesi becerileri de dahil olmak üzere, İnternette araştırmada etkili kullanımı konusunda eğitilecektir.

-Okul, personelin ve öğrencilerin İnternet´ten türetilen materyallerin telif hakkı yasalarına uygun olmasını ve bilgi kaynaklarını kabul etmesini sağlayacaktır.

-Öğrencilere, okudukları ve ya gösterilen bilgilerin doğruluğunu kabul etmeden önce eleştirel düşünmeleri öğretilecektir.

-Çevrimiçi materyallerin değerlendirilmesi, her konuda öğretme ve öğrenmenin bir parçasıdır ve müfredatta bir bütün olarak görülür.

KİŞİSEL CİHAZLARIN VE CEP TELEFONLARININ KULLANIMI

Gençlerin ve yetişkinlerin cep telefonlarının ve diğer kişisel cihazların kullanımı, okul tarafından kararlaştırılacak ve okul Kabul Edilebilir Kullanım veya Cep Telefonu Politikası dahil olmak üzere uygun politikalarda yer alacaktır.

1-Kişisel cihazların ve cep telefonlarının güvenli bir şekilde kullanılması için beklentiler

-Kişisel cihazların ve cep telefonlarının kullanımı yasaya ve diğer uygun okul politikalarına uygun olarak yerine getirilecektir.

-Sahaya getirilen her türlü elektronik cihazın sorumluluğu kullanıcıya aittir. Okul, bu tür öğelerin kaybı, çalınması veya zarar görmesi konusunda sorumluluk kabul etmez. Okul, bu tür cihazların potansiyel veya fiili neden olduğu olumsuz sağlık etkileri için sorumluluk kabul etmez.

Kötüye kullanım veya uygun olmayan mesajların veya içeriğin cep telefonları veya kişisel cihazlarla gönderilmesi, topluluğun herhangi bir üyesi tarafından yasaklanır ve herhangi bir ihlal, disiplin / davranış politikasının bir parçası olarak ele alınacaktır.

Topluluğunun tüm üyelerine cep telefonlarını veya cihazlarını kayıp, hırsızlık veya hasardan korumak için adım atmaları önerilir.

Topluluğunun tüm üyelerinden, kayboldukları veya çalındığı takdirde yetkisiz aramaların veya hareketlerin telefonlarında veya cihazlarında yapılamayacağından emin olmak için şifreler / pin numaraları kullanmaları önerilir. Parolalar ve pin numaraları gizli tutulmalıdır. Cep telefonları ve kişisel cihazlar paylaşılmamalıdır.

2-Öğrencilerin kişisel cihazlarını ve cep telefonlarını kullanımı

-Öğrenciler, kişisel cihazların ve cep telefonlarının güvenli ve uygun kullanımı konusunda eğitim alacaklardır.

-Bilişim araçlarını, okul yönetimi ile öğretmenin bilgisi ve izni dışında konuşma yaparak, ses ve görüntü alarak, mesaj ve e-mail göndererek, bunları arkadaşlarıyla paylaşarak eğitim-öğretimi olumsuz yönde etkileyecek şekilde kullanmak aynı zamanda okul ders saatleri içerisinde telefon bulundurmak kesinlikle yasaktır.

-Çocukların cep telefonlarının ve kişisel cihazların tüm kullanımları, kabul edilebilir kullanım politikasına uygun olarak gerçekleşecektir.

-Cep telefonları veya kişisel cihazlar, müfredat tabanlı etkinlik kapsamında olmadıkları sürece dersler veya resmi okul saatlerinde öğrenciler tarafından kullanılamaz.

-Çocukların cep telefonlarını veya kişisel cihazlarını eğitim etkinliğinde kullanımı, okul idaresi tarafından onaylandığında gerçekleşecektir.

-Bir öğrenci ebeveynlerini arama gereği duyduğunda, okul telefonunu kullanmasına izin verilecektir.

-Ebeveynlerin okul saatlerinde cep telefonuyla çocuklarıyla iletişim kurmamaları, okul idaresine başvurmaları önerilir. İstisnai durumlarda öğretmenin onayladığı şekilde istisnalara izin verilebilir.

-Öğrenciler, telefon numaralarını yalnızca güvenilir arkadaşlarına ve aile üyelerine vermelidirler.

-Öğrencilere, cep telefonlarının ve kişisel cihazların güvenli ve uygun bir şekilde kullanımı öğretilecek ve sınırların ve sonuçların farkına varılacaktır.

3-Ödül Ve Disiplin Yönetmeliği Cep Telefonu İle İlgili Maddeler

Disiplin cezasını gerektiren davranışlar:

MADDE 12 – (1) Cezayı gerektiren davranışlar şunlardır:

a) Kınama cezasını gerektiren davranışlar; 18) Bilişim araçlarını, okul yönetimi ile öğretmenin bilgisi ve izni dışında konuşma yaparak, ses ve görüntü alarak, mesaj ve e-mail göndererek, bunları arkadaşlarıyla paylaşarak eğitim-öğretimi olumsuz yönde etkileyecek şekilde kullanmak,

b) Okuldan kısa süreli uzaklaştırma cezasını gerektiren davranışlar; 8) Bilişim araçları ile yönetici, öğretmen, eğitici personel, memur, diğer görevliler ve ziyaretçiler ile öğrencileri rahatsız edici davranışlarda bulunmak,

c) Okuldan tasdikname ile uzaklaştırma cezasını gerektiren davranışlar; 14) Bilişim araçları ile yönetici, öğretmen, eğitici personel, öğrenci, memur, diğer görevliler ve ziyaretçilere etik olmayan ses, söz ve görüntülerle zarar verici davranışlarda bulunmak,

ç) Örgün eğitim dışına çıkarma cezasını gerektiren davranışlar; 14) Bilişim araçları ile toplum değerlerine aykırı zararlı, bölücü, yıkıcı, ahlak dışı ve şiddet içerikli yasak yayınlar bulundurarak kişi ve kurumlarla ilgili ses, söz ve görüntüler alıp bunları çoğaltmak, sanal ortamlarda dinlemek, dinlettirmek, izlemek, izlettirmek, yaymak ve ticaretini yapmak,"

Görüldüğü üzere cep telefonunun yanlış amaçlar doğrultusunda kullanımı ile ilgili yönetmelik maddeleri açık olup, bu konuda velilerimizin gerekli uyarı ve tavsiyeleri öğrencilerine duyurmaları önemle rica olunur.

4-Personelin kişisel cihazlar ve cep telefonları kullanımı

-Personel, çocukların fotoğraflarını veya videolarını çekmek için cep telefonları, tabletler veya kameralar gibi kişisel cihazları kullanmaz ve yalnızca bu amaçla işle sağlanan ekipmanı kullanır.

-Personel herhangi bir kişisel cihazı doğrudan çocuklarla kullanmaz ve ders / eğitim etkinlikleri sırasında yalnızca okul tarafından sağlanan ekipmanı kullanır.

-Personel kişisel cep telefonları ve cihazları ders saatlerinde kapatılıp / sessiz moda geçirilir.

-Bluetooth veya diğer iletişim biçimleri ders saatlerinde "gizlenmiş" veya kapalı olmalıdır.

-Acil durumlarda okul idaresi tarafından izin verilmemişse, kişisel cep telefonları veya cihazları öğretim dönemleri boyunca kullanılamaz.

-Bir personel okul politikasını ihlal ettiği durumlarda disiplin işlemi yapılır.

-Bir personelin, bir cep telefonuna veya kişisel bir cihaza kaydedilen veya saklanan yasadışı içeriğe sahip olduğu veya ceza gerektiren bir suç işlemiş olması durumunda, polise ulaşılacaktır.

5-Ziyaretçiler kişisel cihazların ve cep telefonlarının kullanılması

-Ebeveynler ve ziyaretçiler, okulun kabul edilebilir kullanım politikasına uygun olarak cep telefonlarını ve kişisel cihazları kullanmalıdır.

-Fotoğraflar veya videolar çekmek için ziyaretçiler ve ebeveynler tarafından cep telefonlarının veya kişisel cihazların kullanılması, okul resim kullanımı politikasına uygun olarak gerçekleştirilmelidir.

-Okul, ziyaretçilere kullanım beklentilerini bildirmek için uygun tabela ve bilgileri sağlayacak ve sunacaktır.

SİBER ZORBALIK

Siber zorbalık nedir?

Bir ya da birden fazla kişinin elektronik iletişim araçlarını kullanmak suretiyle belirli bir zaman içerisinde ve sürekli olarak, kendisini savunma gücüne sahip olmayan bir kişiye yönelik gerçekleştirilen kasıtlı saldırgan davranışlardır.

Siber zorbalık davranışları nasıl gerçekleştirilmekte?

Bu davranışların başında zorbanın, kurbanı, elektronik iletişim araçları yoluyla tehdit etmesi ya da kurbana yönelik kötü sözler içeren mesajlar göndermesi gelmektedir. Bazen de mağdur hakkında internet ortamında dedikodu yaparak ya da mağduru rahatsız edecek özel resim ve bilgiler yayma yoluyla gerçekleştirilmektedir. Yaygın siber zorbalık davranışlarından biride zorbanın internet ortamından kendisini mağdur gibi tanıtıp onun adına başkalına zorbalık yapmasıdır. Bu tür davranışlar, mağdurun cep telefonu ya da elektronik posta hesabını kullanarak

gerçekleştirdiği görülmektedir. Bunlara ek olarak isimsiz çağrılar, virüslü e-postalar ve bir kişi ya da bir grubu karalamak için kısa mesaj ya da e-postaların gönderilmesi de diğer siber zorbalık davranışları arasında yer almaktadır.

İki çeşit siber zorbalık bulunmaktadır.

Elektronik zorbalık: Olayın daha çok teknik yönünü içermektedir. Bu zorbalık kişilerin şifrelerini ele geçirmek, web sitelerini heklemek, spam içeren mailler göndermek ya da bulaşıcı mailler göndermek gibi teknik olayları içerir. Bireysel yapılabileceği gibi birçok kişi tarafından organize bir şekilde aynı anda da yapılabilir.

E-iletişim zorbalığı: Olayın daha çok psikolojik yönünü içerir. Bilgi ve iletişim teknolojilerini kullanarak kişileri sürekli rahatsız etme, isim takma, dedikodu yapma internet üzerinden kişiye hakaret etme ya da kişinin rızası olmadan fotoğraflarını yayınlama gibi ilişkisel saldırı davranışlarını içerir.

ÇOCUKLARIN VE GENÇLERİN KATILIMI VE EĞİTİMİ

-Öğrenciler arasında güvenli ve sorumlu internet kullanımının önemi ile ilgili farkındalık yaratmak için bir çevrimiçi güvenlik (e-Güvenlik) müfredatı oluşturulur ve okulun tamamında yer alır.

-Güvenli ve sorumlu kullanım ile ilgili eğitim internet erişiminden önce yapılacaktır.

-Müfredat geliştirme ve uygulama da dahil olmak üzere okul çevrimiçi güvenlik politikaları ve uygulamaları yazarken ve geliştirirken öğrenci katkıları aranacaktır.

-Tüm kullanıcılara ağ ve internet kullanımının izleneceği bildirilecektir.

-Çevrimiçi güvenlik (e-Güvenlik) PSHE, SRE, Citizenshipand Computing / BİT programlarına dahil edilecek ve hem güvenli okul hem de evde kullanımını kapsayacaktır.

-İnternetin ve teknolojinin güvenli ve sorumlu kullanımı, müfredatta ve tüm konularda güçlenecektir. Öğretmenler Kurulu, Zümre Öğretmenler ve Şube Öğretmenler Kurullarında e-Güvenlik Konusu ele alınacak ve konuya gereken hassasiyet gösterilecektir.

-Okul, öğrencilerin teknolojiyi olumlu şekilde kullandıklarını ödüllendirecektir.

-Okul, öğrencilerin ihtiyaçlarına uygun olarak çevrimiçi güvenliği geliştirmek için akran eğitimini uygulayacaktır.

1-Personelin katılımı ve eğitimi

-Çevrimiçi güvenlik (e-Güvenlik) politikası, tüm çalışanların katılımı için resmi olarak sağlanacak ve tartışılacak ve korunma sorumluluğumuzun bir parçası olarak güçlendirilecek ve vurgulanacaktır.

-Çalışanların tüm üyeleri, çevrimiçi davranışlarının okuldaki rolü ve itibarını etkileyebileceğinin farkına varacaktır. Mesleği veya kurumu çürüme durumuna düşürdüğü veya profesyonel yeteneklerine güvenini kaybetmiş bir şeyin bulunduğu düşünülürse, kamusal, disiplin veya hukuki önlemler alınabilir.

-Filtreleme sistemlerini yönetme veya BİT kullanımını izleme sorumluluğu taşıyan personelin üyeleri, Liderlik Ekibi tarafından denetlenecek ve sorunları veya endişeleri bildirmek için açık prosedürlere sahip olacaklar.

-Okul, çalışanların öğrencilerin yaşlarına ve yeteneklerine göre kullanması gereken yararlı çevrimiçi araçları vurgulamaktadır.