# Silifke Kırobası Ortaokulu e-Güvenlik Politikası

## Çevrimiçi Güvenlik Etik Kuralları Oluşturma
## Amaçlar ve politika kapsamı
## Olası beyanlar:

- Silifke Kırobası Ortaokulu, çevrimiçi güvenliğin (e-Güvenlik), bilgisayarlar, tabletler, cep telefonları veya oyun konsolları gibi teknolojiyi kullanırken, dijital dünyadaki çocukların ve yetişkinlerin korunması için vazgeçilmez bir unsur olduğuna inanmaktadır.
- Silifke Kırobası Ortaokulu, internetin ve bilgi iletişim teknolojilerinin günlük yaşamın önemli bir parçası olduğunu belirtir. Dolayısıyla, riskleri yönetmek ve bunlara tepki vermek için
  stratejiler geliştirmenin yollarını öğrenmek ve çevrimiçi ortamda esneklik kazanmak için güç sahibi olmak için çocuklar desteklenmelidir.
- Silifke Kırobası Ortaokulu, eğitim standartlarını yükseltmek, başarıyı teşvik etmek, personelin mesleki çalışmalarını desteklemek ve yönetim işlevlerini geliştirmek için toplumun kaliteli İnternet erişimi sunma yükümlülüğüne sahiptir.
- Silifke Kırobası Ortaokulu, tüm çocukların ve personelin çevrimiçi olarak potansiyel zararlardan korunmasını sağlamakla sorumludur.
- Silifke Kırobası Ortaokulu çevrimiçi güvenlik politikasının amacı şudur:
  - < Silifke Kırobası Ortaokulu güvenli ve güvenli bir ortam olduğundan emin olmak için, toplumun tüm üyelerinden beklenen ana ilkeleri, güvenli ve sorumlu kullanım teknolojisi ile ilgili olarak tanımlamak.
  - Silifke Kırobası Ortaokulu topluluğunun tüm üyelerini çevrimiçi olarak korumak ve güvenliğini sağlamak.
  - Teknolojinin potansiyel riskleri ve yararları konusunda Silifke Kırobası Ortaokulu 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, yönetim organı, öğretmenler, destek personeli, harici yükleniciler, ziyaretçiler, gönüllüler ve okul adına hizmet veren veya bunları yerine getiren diğer kişiler (toplu olarak bu politikada 'personel' olarak anılacaktır) dâhil olmak üzere tüm personel için geçerlidir ) yanı sıra çocuklar ve ebeveynler.
- Bu politika, internet erişimi ve kişisel cihazlar da dâhil 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.

- Okul, yerel ve ulusal destek dâhil olmak üzere çevrimiçi güvenlik endişeleri ile ilgili olarak erişmek için okul / çevre topluluğu için sağlam raporlama kanallarının bulunmasını sağlamak.
- Cihazların güvenli ve sorumlu kullanılmasını sağlamak da dâhil olmak üzere, teknolojinin güvenli kullanımı ile ilgili uygun risk değerlendirmelerinin yapılmasını sağlamak.
- Yönetim Organının üyesi olan çevrimiçi güvenliğin sağlanmasına ilişkin sorumluluk üstlenecek bir kişinin sağlanması.
- İyileştirme güç ve alanlarını belirlemek için mevcut çevrimiçi güvenlik uygulamasını denetlemek ve değerlendirmek.
- Belirlenmiş Koruyucu Liderin (DSL), çevrimiçi güvenlik sorumlusu ile birlikte çalışmasını sağlamak.

### 1.2.2 Belirlenmiş Koruyucu Liderin temel sorumlulukları şunlardır:

- Tüm çevrimiçi korunma konularında adlandırılmış bir irtibat noktası olarak hareket etmek ve diğer personel üyeleri ve diğer ajanslarla uygun şekilde iletişime geçmek.
- Çevrimiçi güvenlikle ilgili mevcut araştırma, mevzuat ve eğilimlerle güncel tutmak.
- Olumlu çevrimiçi davranışı teşvik etmek için yerel ve ulusal etkinliklere katılımı koordine etmek, örneğin Güvenli İnternet Günü.
- Çevrimiçi güvenliğin çeşitli kanallar ve yaklaşımlar vasıtasıyla ebeveynlere ve daha geniş topluluğa tanıtılmasını sağlama.
- Çevrimiçi güvenlik olaylarının ve kayıt yapılarını ve mekanizmalarını koruyan okulların bir parçası olarak alınan önlemlerin kayıtlarını tutmak.
- Okul yönetim ekibine ve diğer birimlere, çevrimiçi güvenlik sorunları ve yerel veriler / rakamlar hakkında rapor vermek.
- Yerel ve ulusal kurumlarla irtibat kurmak.
- Paydaş katkısı ile düzenli olarak çevrimiçi güvenlik politikalarını, Kabul Edilebilir Kullanım Politikalarını (AUP'ler) ve diğer ilgili politikaları gözden geçirmek ve güncellemek için okul / liderlik ve yönetimle birlikte çalışmak.
- Çevrimiçi güvenliğin diğer uygun okul politikaları ve prosedürleriyle bütünleştirilmesini sağlamak.

### 1.2.3 Tüm çalışanların kilit sorumlulukları şunlardır:

- Çevrimiçi güvenlik politikalarının geliştirilmesine katkıda bulunmak.
- Kabul Edilebilir Kullanım Politikalarını (AUP'lar) okumak ve onlara bağlı kalmak.
- Okul / ortam 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.
- Çevrimiçi güvenlik konusunu ne zaman ve ne kadar içte ve dışta tırmanacağınızı bilmek.

- 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.

### 1.2.6 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.

# 1. Çevrimiçi İletişim ve Teknolojinin Daha Güvenli Kullanımı

## 1.1 Okul / web sitesinin yönetilmesi

### Olası beyanlar:

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

- Okul, çevrimiçi güvenlik dâhil olmak üzere, toplumun üyeleri için okul web sitesinde korunma hakkında bilgi gönderecektir.

İçerik

- Bir video konferans dersi kaydederken, tüm siteler ve katılımcılar tarafından yazılı izin alınacaktır. Konferansın başlangıcında kayıt nedeni belirtilmeli ve video konferans kaydı tüm taraflara açık olmalıdır. Kaydedilen malzemeler güvenli bir şekilde saklanacaktır.
- Üçüncü taraf materyalleri dâhil edilecekse, okul üçüncü şahsın fikri mülkiyet haklarını ihlal etmekten kaçınmak için bu kaydın kabul edilebilir olup olmadığını kontrol edecektir.
- Okul, bir video konferansa katılmadan önce diğer konferans katılımcılarıyla diyalog kuracak. Okul değilse, okul sınıf için uygun olan materyali teslim aldığını kontrol edecektir.

## 2.4 İnternetin ve ilgili cihazların uygun ve güvenli derslik kullanımı
## 2.4 Olası beyanlar:

- İnternet kullanımı eğitimsel erişimin önemli bir özelliğidir ve tüm çocuklar bütünleşik okul müfredatının bir parçası olarak sorunlarını yanıtlamak için stratejiler geliştirmelerini destekleyecek ve onlara yardımcı olacak yaşa ve yeteneğe uygun eğitim alacaklardır. Daha fazla bilgi için lütfen özel müfredat politikalarına erişin.
- Okulun / ortamın 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.
- Öğrencilerin yaşlarına ve yeteneklerine uygun olacaktır.
    - Genç öğrencilerin İnternet'e erişimi, yetişkinlerin gösteri yaparak, öğrencilerin yaşı ve yeteneği için planlanan öğrenme çıktılarını destekleyen belirli ve onaylanmış çevrimiçi materyallere doğrudan denetlenen erişimle sağlanacaktır.
    - 8-11 yaşındaki öğrenci denetlenecek. Öğrenciler yaşa uygun arama motorlarını ve çevrimiçi araçları kullanacak ve çevrimiçi etkinlikler gerektiğinde öğretmen tarafından yönlendirilecek. Çocuklar, öğrencilerin yaşı ve yeteneği için planlanan öğrenme çıktılarını destekleyen çevrimiçi materyal ve kaynaklara yönlendirilecektir.
    - Yetenek ve anlayışlarına göre, genç öğrenciler teknoloji kullanırken uygun bir şekilde gözetim altına alınacaklardır.
- 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 dâhil 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.

- Silifke Kırobası Ortaokulu topluluğunun tüm üyelerine, cep telefonlarının ve kişisel cihazlarının saldırgan, küçümseyen veya başka şekilde okul/ayar politikalarına aykırı düşen herhangi bir içerik içermediğinden emin olmaları önerilir.

## 3.3 Öğrencilerin kişisel cihazlarını ve cep telefonlarını kullanımı
## 3.3 Olası Bildirimler:

- Öğrenciler, kişisel cihazların ve cep telefonlarının güvenli ve uygun kullanımı konusunda eğitim alacaklardır.
- Çocukların cep telefonlarının ve kişisel cihazların tüm kullanımları, kabul edilebilir kullanım politikasına uygun olarak gerçekleşecektir.
- Cep telefonları veya kişisel cihazlar, öğrencilerin bir öğretim üyesinin onayını alarak onaylanmış ve yönlendirilmiş 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.
- Öğrencinin kişisel cihazında veya cep telefonunda bulunan materyalin yasadışı olabileceği veya cezai bir suçla ilgili kanıt sağlayabileceğinden şüpheleniliyorsa, cihaz daha ayrıntılı araştırma için polise teslim edilir.

## 3.4 Kişisel cihazların ve cep telefonlarının personel kullanımı
## 3.4 Olası Bildirimler:

- Personelin, kendi kişisel telefonlarını veya cihazlarını, çocukların, gençlerin ve ailelerinin, mesleki bir kapasitede, ortamın içinde veya dışındaki bölgeleriyle bağlantı kurmalarına izin verilmez. Bu konuyu tehlikeye atacak önceden var olan ilişkiler yöneticilerle görüşülecektir.
- 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.

- Okul, kullanıcıların yalnızca uygun materyallere erişmesini sağlamak için makul önlemleri alacaktır. Bununla birlikte, internet içeriğinin küresel ve bağlanmış niteliğinden dolayı, uygun olmayan materyallerin bir okul/bilgisayar ya da cihaz vasıtasıyla hiçbir zaman gerçekleşmeyeceğini garanti etmek her zaman mümkün değildir.
- Okul, çevrimiçi güvenlik (e-Güvenlik) politikasının yeterli olup olmadığını ve politikanın uygulanmasının uygun olup olmadığını belirlemek için teknolojinin kullanımını denetleyecektir.
- Çevrimiçi riskleri belirleme, değerlendirme ve azaltma yöntemleri okul liderliği ekibi tarafından düzenli olarak incelenecektir.

## 4.2. Daha geniş çapta okul / toplum ortamında internet kullanımı
## 3.2 Olası beyanlar:

- Okul, çevrimiçi güvenlik konusunda ortak bir yaklaşım oluşturmak için yerel kuruluşlarla irtibat kuracak.
- Okul, internet kullanımının uygun olmasını sağlamak için yerel topluluğun ihtiyaçları (kültürel geçmişleri, dilleri, dinleri ve etnik kökenleri tanımayı da içeren) ile çalışacaktır.
- Okul, okul bilgisayar sistemine veya sitedeki internete erişmesi gereken herhangi bir konuk / ziyaretçi için Kabul Edilebilir Kullanım Politikası sağlayacaktır.

## 3.3 İnternet erişiminin yetkilendirilmesi
## 4.3 Olası beyanlar:

- Okul, okulun cihaz ve sistemlerine erişim izni verilen tüm personelin ve öğrencilerin güncel bir kaydını tutacaktır.
- Tüm personel, öğrenciler ve ziyaretçiler, herhangi bir okul kaynaklarını kullanmadan önce Kabul Edilebilir Kullanım Politikasını okuyacak ve imzalayacaklardır.
- Ebeveynlere, öğrencilere, yaşlarına ve yeteneklerine uygun denetlenen İnternet erişimi sağlanacakları bildirilecektir.
- Ebeveynlerden, öğrencilerin erişebilmesi için Kabul Edilebilir Kullanım Politikasını okumaları ve uygun olduğunda, çocuklarıyla tartışmaları istenecektir.
- Toplumun savunmasız üyeleri için (özel eğitim gereksinimi olan çocuklar gibi) erişimi düşünürken, okul öğrencilerin belirli ihtiyaçları ve anlayışları temelinde kararlar alacaktır.

- 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.

## 5.4 Ebeveynlerin katılımı ve eğitimi

## 5.4 Olası beyanlar:

- Silifke Kırobası Ortaokulu, çocukların internetin ve dijital teknolojinin güvenilir ve sorumlu kullanıcıları olabilmesi için ana-babaların oynayacakları önemli bir role sahip olduklarını kabul eder.
- Ebeveynlerin dikkatleri, okul açıklamaları ve okul web sitesinde okul çevrimiçi güvenlik (e-Güvenlik) politikasına ve beklentilerine yönelecektir.
- Okul Anlaşması'nın bir parçası olarak ebeveynlerin çevrimiçi güvenlik bilgilerini okumaları istenecektir.
- Ebeveynler, Okula Kabul Edilebilir Kullanım Politikası'nı okumaya ve çocuklarıyla etkilerini tartışmaya teşvik edilecektir.
- Çevrimiçi güvenlik konusundaki ebeveynler için bilgi ve rehberlik, ebeveynlere çeşitli biçimlerde sunulacaktır.
- Ebeveynlerin, çevrimiçi olarak çocukları için olumlu davranışları rol modellemeleri teşvik edilecektir.

**ÇevrimiçiOlaylaraveKorumasorunlarınayanıtverme**
**Olası beyanlar:**

- Okulun tüm üyeleri, cinsel içerikli mesajlaşma, çevrimiçi / siber zorbalık vb. dâhil olmak üzere karşılaşılabilecek çevrimiçi risklerin çeşitliliğinden haberdar edilecektir. Bu, öğrencilere yönelik personel eğitimi ve eğitim yaklaşımları içerisinde vurgulanacaktır.
- Okulun tüm üyeleri, filtreleme, cinsel içerikli mesajlaşma, siber zorbalık, yasadışı içerik ihlali vb. Gibi çevrimiçi güvenlik (e-Güvenlik) endişelerini bildirme prosedürü hakkında bilgilendirilecektir.
- Dijital Abone Hattı (DSL), daha sonra kaydedilecek olan çocuk koruma endişelerini içeren herhangi bir çevrimiçi güvenlik (e-Güvenlik) olayı hakkında bilgilendirilecektir.
- İnternet'in yanlış kullanımı ile ilgili şikâyetler, okulun şikâyet prosedürleri kapsamında ele alınacaktır.
- Çevrimiçi / siber zorbalık ile ilgili şikâyetler, okulun zorbalık karşıtı politikası ve prosedürü kapsamında ele alınacak