

# e-Güvenlik (e-Safety) POL T KASI



**KAD R HAS LKOKULU**  
**e-Güvenlik (e-Safety) POL T KASI**  
**ve**  
**AMAÇLARI**

Teknolojinin hızla gelişmesiyle birlikte her okulun Okul Güvenlik Politikasının olması kaçınılmaz olmuştur. Çünkü paydaşlar günümüzde okul binasından çok çeşitli şekillerde internete erişebilirler. Günlük hayatımızın bir parçası olarak hepimiz dijital teknolojilerle yaşıyoruz. Çocuklarımızın dijital teknolojiler aracılığıyla mevcut olan fırsatları en iyi nasıl kullanacaklarını bilmelerini sağlamak için, artık bunları nasıl kullanacaklarını bilmek ve anlamak gerekiyor. Bunun mümkün olan en güvenli şekilde ve en güvenli ortamda yapılmasını sağlamak için, öğrencilerimizin evde, okulda veya dışarıda ya da arkadaşlarıyla ya da yalnız olduğu zaman, dikkatini çeken açık ve özlü bir Güvenli İnternet Okul Politikasına sahip bir okuluz.

## **A. ÖZETLE E-GÜVENLİK (E-SAFETY) POL T KAMIZ:**

1. Okulumuzun internet sitesi, twitter gibi sosyal ağları bulunmaktadır. Bu ağların üzerinde yayınlanan veriler kontrollü olarak paylaşılmaktadır.
2. Okulumuzda cep telefonları ders esnasında kapalı konumda tutulmakta, eTwinning projesi yapan arkadaşlar proje çalışmalarını amacıyla gerektiği takdirde kullanmaktadır.
3. Rehberlik servisi tarafından, sınıflara düzenli olarak, B T bağımlılığı, B T'nin doğru ve güvenli kullanımı, Siber Zorbalık gibi konularda seminerler tertiplenmektedir.
4. Okulumuzda B T doğru ve güvenli kullanımı ile ilgili sabit panolar bulunmaktadır.
5. Okulumuzun bazı öğretmenleri Milli Eğitim Bakanlığı tarafından verilen Siber Zorbalık, B T'nin doğru ve güvenli kullanımı konularında uzaktan ve yüz yüze eğitimler almıştır.
6. Okulumuzda "Daha Güvenli İnternet Günü" kutlanmaktadır.
7. Okulumuzun internet sitesinde e-güvenlik konusunda, güvenliweb.org.tr. sitesi linki yer almaktadır. Okul paydaşlarımız istedikleri zaman konu ile ilgili bilgi alabilmekteler.

8. Okulumuzda güvenli internet günü kutlamalarında, konu ile ilgili seminerlerde güvenliweb.org.tr. sitesinden alıntılanan bilgi broürleri dağıtılmaktadır.
9. Rehber Öğretmenlerimiz internet etiği ve güvenli internet kullanımı konuları hakkında öğrencilerimize bilgilerini aktarmaktadır.
10. Okulumuzda 21.yy iletişim becerileri önemsenmektedir. Bununla ilgili olarak öğrencilerimizin B T kullanım becerilerini geliştirme çabaları yapılmaktadır.
11. Okulumuzda Dijital vatandaş olma konusunda paydaşlarımızı bilinçlendirme çabaları yapılmaktadır.

## **B. OKULUMUZDA E-GÜVENLİK POLİTİKASININ AMACI;**

OKULUMUZ'un tüm üyelerini çevrimiçi olarak korumak ve güvenliğini sağlamak.

Teknolojinin potansiyel riskleri ve yararları konusunda KADINLAR HASTALIKLARI İDARECİ, öğretmeni öğrenci ve çalışanları için 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 politikanın, 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) dahil olmak üzere tüm personel için geçerlidir ) yanı sıra çocuklar ve ebeveynleri kapsamını sağlamak,

Sonuç olarak ana hedefimiz, internet erişimi ve kişisel cihazlar da dahil olmak üzere bilgi iletişim cihazlarının kullanımı için bu güvenlik politikasının geçerli olmasıdır.; 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 KİMLİK SORUMLULUKLARI UNLARDIR:**

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 iletişimlenebileceklerini 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 endişeye duyan bireylerin belirlenmesi ve uygun önlem alınması.

Olumlu öğrenme fırsatlarına vurgu yapmak.

Bu alanda mesleki gelişim için kişisel sorumluluk almak.

## **ÇOCUKLARIN VE GENÇLERİN BAĞLI SORUMLULUKLARI UNLARDIR:**

Çevrimiçi güvenlik politikalarının geliştirilmesine katkıda bulunmak.

Okulun Kabul Edilebilir Kullanım Politikalarını okumak ve onlara bağlı kalmak.

Çevrim içi ve çevrim dışı bağlanmalarının hislerine ve haklarına saygı duymak.

Her ters giderse, güvenilir bir yetkenden yardım istemek ve çevrimiçi güvenlik sorunlarıyla karışık diğer kişileri desteklemek.

## **Bireysel yeteneklerine ve zayıf yönlerine uygun bir seviyede:**

Kendilerini ve bakalarını 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.

## **EBEVEYNLERİN BAĞIMSIZ SORUMLULUKLARI ŞUNLARDIR:**

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 de işaretleri belirlemek.

Okul veya diğer uygun kurumlardan, kendileri ve ya çocukları çevrimiçi problem veya sorunlarla karşılaşsa yardım veya destek istemek.

Okulun çevrimiçi güvenlik politikalarının oluşturulmasına katkıda bulunmak.

Öğrenme platformları ve diğer araç 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.

## **C. ÇEVİRİMİÇİ İLETİŞİM VE TEKNOLOJİNİN DAHA GÜVENLİ KULLANIMI**

### **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 çalışmalarını öğrencilerin izniyle ya da ebeveynlerinin izniyle yayınlanacaktır.

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

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

### **Çevrimiçi görüntü ve videolar yayınlama**

Okul, çevrimiçi paylaşılan tüm resimlerin ve videoların okul resim kullanımı politikasına uygun şekilde kullanılmasını sağlayacaktır.

Okul, resimlerin ve videoların tümünün, veri güvenliği, Kabul Edilebilir Kullanım Politikaları, Davranış Kuralları, sosyal medya, kişisel cihazların ve cep telefonlarının kullanımı gibi diğer politikalar ve prosedürlere uygun şekilde yer almasını sağlayacaktır.

Görüntü politikasına uygun olarak, öğrencilerin resimlerinin / videolarının elektronik olarak yayınlanmasından önce her zaman ebeveynlerin yazılı izni alınacaktır.

## Video Konferans Kuralları

Ö renciler, bir video konferans araması veya mesajı hazırlamadan veya cevaplamadan önce bir öğretmen'in izni isteyecektir.

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

Velilerin rızası, çocuklar video konferans faaliyetlerine katılmadan önce alınacaktır.

Video konferans, solum bir risk değerlendirilmesini takiben, resmi ve onaylanmış iletişim kanalları vasıtasıyla gerçekleştirilecektir.

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

Etimsel video konferans servisleri için özel oturum açma ve ifre bilgileri yalnızca personellere verilecek ve gizli tutulacaktır.

## Kişisel Cihazların ve Cep Telefonlarının Kullanımı

Cep telefonlarının ve çocukların, gençlerin ve yetişkinler arasındaki diğer kişisel cihazların yaygın bir şekilde sahiplenilmesi, tüm üyelerin cep telefonlarının ve kişisel cihazların sorumlu bir şekilde kullanılmasını sağlamak için gerekli adımları atmalarını gerektirir.

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.

Kadir Has İkokulu, mobil teknolojilerle yapılan kişisel iletişim, çocuklar, personel ve anne-babalar için gündelik yaşamın kabul edilen bir parçası olduğunu farkındadır; ancak, bu tür teknolojilerin okulda güvenli ve uygun bir şekilde kullanılmasını gerektirir.

## Öğrencilerin kişisel cihazlarını ve cep telefonlarını kullanımı

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

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

Öğrenciler ders başlamadan önce telefonlarını okul yönetimi tarafından yaptırılan telefon kutularına koymakla yükümlüdür. Cep telefonunun amacı dışında kullanımı ihlali olduğu anda, öğrenci, telefondaki özel verilerin korunmasını sağlamak amacıyla telefonunu kapatıp ders öğretmenine verir. Ders öğretmeni öğrenci telefonunu ilgili müdür yardımcısına teslim eder. Cep telefonu öğrenci velisine teslim edilmeye kadar güvenli bir yerde tutulur. Velisi dışında telefon kimseye teslim edilmez.

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

Cep telefonları veya kişisel cihazlar, bir öğretmenin 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 onaylanmadıkça gerçekleştirilecektir.

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

Ebeveynlerin okul saatlerinde cep telefonu ile çocuklarıyla iletişim kurmamaları, okul idaresine başvurularını önerilir. İstisnai durumlarda öğretmenin onayladığı şekilde istisnalara izin verilebilir.

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

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

Ö rencinin kişisel cihazında veya cep telefonunda bulunan materyalin yasadışı olabileceği veya cezai bir suçla ilgili kanıt sağlanabileceğinden şüpheleniliyorsa, cihaz daha ayrıntılı araştırma için polise teslim edilir.

### **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 kullanım politikasına uygun olarak gerçekleştirilmelidir.

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

Personelin uygun ve güvenli olduğunda sorunlara karşı çıkması beklenir ve her zaman ziyaretçilerin herhangi bir ihlalinin idareye bildirecektir.

### **Çocukların ve gençlerin katılımı ve eğitim**

Ö renciler 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.

Ö renciler, Kabul Edilebilir Kullanım Politikasını, yaşlarına ve yeteneklerine uygun bir şekilde okumak ve anlamak için desteklenecektir.

Tüm kullanıcılara aile ve internet kullanımının izleneceği bildirilecektir.

Kabul Edilebilir Kullanım beklentileri ve Posterler, İnternet erişimi olan tüm odalarda yayınlanacaktır.

İnternetin ve teknolojinin güvenli ve sorumlu kullanımı, müfredatta ve tüm konularda güçlenecektir.

Destekten destek, okulların dahili çevrimiçi güvenlik (e-Güvenlik) eğitim yaklaşımlarını tamamlamak ve desteklemek için kullanılacaktır.

Okul, öğrencilerin teknolojiyi olumlu şekilde kullandıklarını ödüllendirecektir.

Okul, öğrencilerin ihtiyaçlarına uygun olarak çevrimiçi güvenli eğitimi geliştirmek için akran eğitimini uygulayacaktır.

### **Personelin katılımı ve eğitim**

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

Personel, İnternet trafiğinin izlenebileceğini ve tek bir kullanıcıya kadar izlenebileceğinin farkında olacak. Okul sistemlerini ve cihazlarını kullanırken takdir yetkisi ve profesyonel davranış gereklidir.

Personelin tüm üyelerine, profesyonel ve kişisel olarak güvenli ve sorumlu İnternet kullanımı konusunda güncel ve uygun personel eğitimi, düzenli (en az yıllık) temelde gerçekleştirilecektir.

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

Filtreleme sistemlerini yönetme veya B T kullanımını izleme sorumluluğu taahhüt eden 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.

### **Ebeveynlerin katılımı ve eğitim**

Kadir Has İlkokulu, 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.

Okulumuzun 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.

### **Çevrimiçi Olaylara ve Koruma sorunlarına yanıt verme**

Okulun tüm üyeleri, sakıncalı mesajlaşma, çevrimiçi / siber zorbalık vb. dahil olmak üzere kararlaştırılabilecek çevrimiçi risklerin çeşitliliğinden haberdar edilecektir. Bu, öğrencilere yönelik personel eğitimi ve eğitim yaklaşımları içerisinde vurgulanacaktır.

Okulun tüm üyeleri, filtreleme, sakıncalı 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 şikayetler, okulun şikayet prosedürleri kapsamında ele alınacaktır.

Çevrimiçi / siber zorbalık ile ilgili şikayetler, okulun zorbalık karartı politikası ve prosedürü kapsamında ele alınacaktır.

Personelin yanlış kullanımı ile ilgili herhangi bir şikayet okul müdürüne yönlendirilecektir. Okul şikayet prosedürü öğrencilere, velilere ve personele bildirilecektir.

Şikayet ve ihbar prosedürü personele bildirilecektir.

Okulun tüm üyeleri, gizliliğinin öneminden ve endişeleri bildirmek için resmi okul usullerine uyma ihtiyacından haberdar olmalıdırlar.

Okulun tüm üyeleri, çevrimiçi ortamda güvenli ve uygun davranış hakkında hatırlatılacak ve okul camiasının herhangi bir diğer üyesine zarar vermek, sıkıntı yaratmak veya suç oluşturan herhangi bir içerik, yorum, resim veya video yayımlamamanın önemini hatırlatacaktır.

Okul, çevrimiçi güvenlik (e-Güvenlik) olaylarını, uygun olduğunda, okul disiplini / davranış politikasına uygun olarak yönetir.

Okul, ebeveynlere, ihtiyaç duyulduğunda bunlarla ilgili endişeleri bildirir.

Herhangi bir soru turma tamamlandıktan sonra okul bilgi alacak, öğrenilen dersleri belirleyecek ve derinlikleri gerektiği gibi uygulayacaktır.

Sorunları çözmek için ebeveynlerin ve çocukların okulla ortak çalışması gerekir.