



ŞEHİT SADIK ORTAOKULU OKUL E-GÜVENLİK POLİTİKASI

1. AMAÇ

- Bu politikanın amacı, Şehit Sadık Ortaokulu'nun bilişim teknolojilerinin kullanım koşullarını ve kabul edilebilir kullanım politikasını belirlemektir.
- Şehit Sadık Ortaokulu, e-güvenlik çalışmaları ile internet, akıllı tahta, bilgisayar, diz üstü bilgisayar ve cep telefonlarını kullanırken; öğrencilerin, velilerin ve öğretmenlerin korunmasını amaç edinmiştir.
- Şehit Sadık Ortaokulu, çevrimiçi güvenliğin (e-Güvenlik), bilgisayarlar, tabletler, cep telefonları gibi teknolojiyi kullanırken, dijital dünyadaki çocukların ve yetişkinlerin korunması için vazgeçilmez bir unsur olduğuna inanmaktadır.
- Güvenlik politikamız, öğrenci davranışları, Eğitim Programları, Veri Koruma ve Güvenliği ile zorbalık gibi politikaları içeren diğer politikalarla bağlantılı olarak etkileşim halindedir.

2. KAPSAM

Bu politika, tüm Şehit Sadık Ortaokulu bilgisayar sistemleri ve bilgi teknoloji servislerine okul içinden veya dışından erişim hakkı verilen tüm kullanıcıları kapsar.

3. SORUMLULUKLAR

- Bu politikanın uygulanmasından okul müdürü sorumludur.
- Bu politikanın hazırlanmasından ve güncellenmesinden okul yönetimi ve Bilişim Teknolojileri Öğretmeni sorumludur.
- Tüm çalışanların sorumlulukları şunlardır:
 - ✚ Çevrimiçi güvenlik politikalarının geliştirilmesine katkıda bulunmak.
 - ✚ Kabul Edilebilir Kullanım Politikalarını 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 modellemek.
 - ✚ Mümkün olduğunca müfredat ile çevrimiçi güvenlik eğitimi ilişkilendirmek.
 - ✚ Okul koruma politikalarını ve prosedürlerini takip ederek endişe duyan bireyleri belirlenmek ve önlem alınmak.
 - ✚ Olumlu öğrenme fırsatlarına vurgu yapmak.
 - ✚ Bu alanda mesleki gelişim için kişisel sorumluluk almak.
- Ebeveynlerin 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. O
- ✚ 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 karşılaşırse yardım veya destek istemek.
- ✚ Yeni ve gelişmekte olan teknolojilerin getirdiği fırsatlar ve risklerle ilgili olarak kendi bilinci ve öğrenimlerinden sorumlu olmak.
- ✚ Okulun çevrimiçi güvenlik politikalarının oluşturulmasına katkıda bulunmak.
- ✚ Öğrenme platformları ve diğer ağ kaynakları gibi okul sistemlerini güvenli ve uygun bir şekilde kullanmak.

4. ÇEVİRİMİÇİ İLETİŞİM VE TEKNOLOJİNİN DAHA GÜVENLİ KULLANIMI

4.1. Okul / web sitesinin yönetilmesi

- Şehit Sadık Ortaokulu olarak okul web sitemizde 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.
- Öğrenci çalışmaları öğrencilerin izniyle ya da ebeveynlerinin izniyle yayınlanacaktır.
- Okul, çevrimiçi güvenlik dahil olmak üzere, toplumun üyeleri için okul web sitesinde korunma hakkında bilgi gönderecektir.
- 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.
- Okulumuz web sayfasında güvenli internet ile ilgili bağlantılar yayınlanacaktır.

4.2. Çevrimiçi görüntü ve videolar yayınlama

- Öğrencileri içeren fotoğraflar dikkatlice seçilecek ve öğrencilerin net olarak kimliklerinin tespit edilmesine izin verilmeyecektir.
- Öğrencilerin isimlerinin tamamı okul web sitesinde veya başka herhangi bir web sayfasında kullanılmayacaktır.
- Okulun internet sitesinde e-Twinning projeleri için kullanılan internet sitelerinde öğrencilerin fotoğrafları paylaşılmadan önce, ebeveynlerden veya velisinden yazılı izin belgesi alınacaktır.
- Fotoğraflar yakından ve öğrencinin karşı cephesinden çekilmeyecektir.
- Çalışmalar sadece öğrencinin ebeveynlerinin izni ile yayınlanabilir.

4.3. İnternetin ve ilgili cihazların uygun ve güvenli kullanımı

- 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.
- Okulun internet erişimi eğitimi geliştirmek ve genişletmek için sağlanmıştır.
- Çalışanların tümü, çocukları korumak için tek başına filtrelemeye güvenmeyeceklerinin farkındadır ve gözetim, sınıf yönetimi ve güvenli ve sorumlu kullanım eğitimi önemlidir.
- Okula 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 ön bilgi alacaktır.
- Tüm çalışanlarımız, velilerimiz ve öğrencilerimiz etkili ve verimli çevirim içi materyallerin kullanımı konusunda bilgilendirilecektir.
- Öğrenciler, bilginin konumlanması, alınması ve değerlendirilmesi becerileri de dahil olmak üzere, internette araştırmada etkili kullanımı konusunda eğitilecektir.
- Okul, personelin ve öğrencilerin internetten türetilen materyallerin telif hakkı yasalarına uygun olmasını ve bilgi kaynaklarını kabul etmesini sağlayacaktır.
- Öğrencilere, okudukları veya gösterilen bilgilerin doğruluğunu kabul etmeden önce eleştirel düşünceleri öğretilecektir.
- Öğretmen ve öğrencilerimiz okulda sadece Milli Eğitim Bakanlığının denetimindeki internet ağını kullanabilirler.
- Okulumuz internet ağına MEB SERTİFİKA güvenlik dosyası yüklenmeden internet ağına bağlanılamaz.
- E-güvenlik ve siber zorbalık konuları belli derslerimizin yıllık planlarına dahil edilecek olup, bu konularda yıl içinde öğrencilere bilgi aktarımı devam edecektir.
- Çevrimiçi materyaller öğretme ve öğrenmenin önemli bir parçası olup müfredat içinde aktif olarak kullanılacaktır.
- Güvenli İnternet Günü okulumuzda kutlanmaktadır ve kutlanmaya devam edilecektir.
- E-güvenlik politikamız Milli Eğitim Bakanlığı tarafından yayınlanan güvenli internet çerçevesine dâhildir. (Milli Eğitim Bakanlığı 2017/12 Sayılı Genelge)

4.4. Kişisel cihazların ve cep telefonlarının kullanımı

- Ders saatleri içinde öğrencilerimizin kişisel cep telefonu kullanımı yasaktır.
- Okulumuzda izinsiz fotoğraf çekilemez.
- Her türlü kişisel cihazların sorumluluğu kişinin kendisine aittir.
- Okulumuz bu tür cihazların kullanımından doğacak olumsuz sağlık ve yasal sorumlulukları kabul etmez.
- Okulumuz kişisel cep telefonlarının ve bilişim cihazlarının kayıp, çalınma ve hasardan korunması için gerekli tüm önlemleri alır fakat sorumluluk kişiye aittir.
- Öğrencilerimiz eğitim amaçlı (web 2 araçlarının kullanımı vb) kişisel cihazlarını kullanmak için okul yönetiminden izin almalıdır.
- Öğrencilerimiz cep telefon numaralarını yalnızca güvenilir kişilerle paylaşmaları, tanımadıkları güvenilir bulmadıkları kişilerle cep telefonu gibi kişisel bilgilerini paylaşmamaları gerektiği konusunda bilinçlendirilmektedirler.
- Çalışanlar (öğretmen, idareci, personel vb) kişisel cep telefonlarını ders saatlerinde sessize alarak ya da kapatarak görevlerine devam etmelidir.
- Çalışanlar (öğretmen, idareci, personel vb) okul politikasına aykırı davranışlarda bulunursa disiplin işlemleri başlatılır.
- Kurum çalışanları (öğretmen, idareci, personel vb) ve öğrenciler sosyal medya ya da sohbet programları üzerinden öğrenci ya da kurum çalışanlarından gelecek olan ya da

kendilerinin gönderecekleri her türlü içerik ve mesajlaşmanın hukuki sorumluluğunu taşımaktadır, uygunsuz olabilecek her türlü içerik ve mesajlaşma ivedilikle okul yönetimi ile paylaşılır. Böyle bir duruma mahal vermemek için gereken önlemler alınır.

4.5. 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.

4.6. Çocukların ve gençlerin katılımı ve eğitimi

- 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.
- Müfredat geliştirme ve uygulama da dahil olmak üzere okul çevrimiçi güvenlik politikaları ve uygulamaları yazarken ve geliştirirken öğrenci katkıları aranacaktır.
- Öğrenciler, Kabul Edilebilir Kullanım Politikasını, yaşlarına ve yeteneklerine uygun bir şekilde okumak ve anlamak için desteklenecektir.
- Tüm kullanıcılara ağ ve internet kullanımının izleneceği bildirilecektir.
- İnternetin ve teknolojinin güvenli ve sorumlu kullanımı, müfredatta ve tüm konularda güçlenecektir.

4.7. Personelin katılımı ve eğitimi

- Okul idaresi ve rehber öğretmenler tarafından dönem başında ve sonunda personellerle düzenli toplantılar yapmaktadır. Toplantı konuları; sosyal medya kullanımı, öğrencilerin sosyal medya kullanımında karşılaştıkları problemlerle nasıl başa çıkabilecekleri ve öğrencilerin fotoğraflarını kullanırken dikkatli olmaları gereken konular hakkında olmaktadır.
- Çevrimiçi güvenlik (e-Güvenlik) politikası, tüm çalışanların katılımı için resmi olarak sağlanacak ve tartışılacak ve korunma sorumluluğumuzun bir parçası olarak güçlendirilecek ve vurgulanacaktır.
- Personel, internet trafiğinin izlenebileceğini ve tek bir kullanıcıya kadar izlenebileceğini farkında olacak. Okul sistemlerini ve cihazlarını kullanırken takdir yetkisi ve profesyonel davranış sergileyeceklerdir.
- Personel, 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.

4.8. Ebeveynlerin katılımı ve eğitimi

- Okul idaresi ve rehber öğretmenler ebeveynleri veli toplantılarında bilgilendirir. Onları, sosyal ağlarda güvende olmak, güçlü bir şifre oluşturmak, E Twinning sayfalarında ve diğer sosyal ağ sitelerinde öğrencilerin fotoğraflarını kullanmak ve mobil cihazların kullanımı hakkında bilgilendirir. Bunun yanında, sınıf öğretmenleri WhatsApp ve sosyal medya grupları hakkında ebeveynlerin bilgilerini sürekli tazeler. Ayrıca, okul politikamızın bir parçası olarak okul e-güvenlik ekibi okulun internet sayfasında egüvenlik hakkında bilgi ve belgeler yayınlar.

- Şehit Sadık Ortaokulu gençlerin internetin ve dijital teknolojinin güvenilir ve sorumlu kullanıcıları olabilmesi için ana-babaların oynayacakları önemli bir role sahip olduklarını kabul eder.
- Ebeveynler, Okula Kabul Edilebilir Kullanım Politikasını okumaya ve çocuklarıyla etkilerini tartışmaya teşvik edilecektir.
- Ebeveynlerin, çevrimiçi olarak çocukları için olumlu davranışları rol modellemeleri teşvik edilecektir.

4.12.Çevrimiçi Olaylara ve Koruma

- Okulumuzun tüm üyeleri çevrim içi riskler konusunda bilgilendirilecektir. Eğitimler yapıp içerikler açıklanacaktır.
- Okulumuzda yasadışı içerik, güvenlik ihlali, siber zorbalık, cinsel içerikli mesajlaşma, çocuk istismarı, kişisel bilgi güvenliği gibi konularda bilgilendirme çalışmaları yapılacaktır.
- İnternetin 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 alınacaktır.
- Okul şikâyet ve ihbar prosedürü öğrencilere, velilere ve personele bildirilecektir.
- Okul, çevrimiçi güvenlik (e-Güvenlik) olaylarını, okul disiplini / davranış politikasına uygun olarak yönetir.
- Sorunları çözmek için ebeveynlerin ve çocukların okulla ortak çalışması gerekmektedir.