ŞEHİT OSMAN DEMİR İLKOKULU E-GÜVENLİK OKUL POLİTİKASI

AMAÇ

- Şehit Osman Demir İlkokulu, e-güvenlik çalışmaları ile internet, bilgisayar, diz üstü bilgisayar ve cep telefonlarını kullanırken; öğrencilerin, velilerin ve öğretmenlerin korunmasını amaç edinmiştir.
- İnternetin ve teknolojinin yaşamın önemli bir parçası olması sebebiyle, herkes, riskleri yönetme ve strateji geliştirme yöntemlerinin öğrenilmesi konusunda bilinçlendirilmelidir.
- Politikamız, yöneticiler, öğretmenler, veliler, tüm personel ve öğrenciler için hazırlanmış olup, internet erişimi ve bilgi iletişim cihazlarının kullanımı için geçerlidir.

SORUMLULUKLAR

- ✓ E-güvenlik politikalarının gelişmesine katkıda bulunmak.
- ✓ Olumlu öğrenme aşamasında gelişim için sorumluluk almak.
- ✓ Okulu ve içerisindekileri korumak içine-güvenlik konusunda sorumluluk almak.
- ✓ Teknolojiyi güvenli ve sorumlu kullanmak.
- ✓ Zarar görülmesi durumunda tehlikeyi gözlemleyip ilgili birimlere iletmek.

OKUL WEB SİTESİ

- ❖ Şehit Osman Demir İlkokulu olarak web sitemizde okulumuzun adres, telefon, fax ve eposta adres bilgileri bulunmaktadır.
- ❖ Sitemizde yayınlanan tüm içerikler okul müdürümüzün onayından geçtikten sonra yetkili okul yöneticimiz tarafından siteye konulmaktadır.
- ❖ Okulumuzun web sitesi ilgili müdür yardımcımızın sorumluluğunda olup güçlü güvenlik önlemleri alınmış durumdadır.
- ❖ Öğrenci çalışmaları, velilerinin izinleriyle yayınlanmaktadır.

GÖRÜNTÜ VE VİDEOLARIN PAYLAŞIMI

- Paylaşılan tüm fotoğraf ve videolar okul politikasına uygun şekilde okul idaresinin izni ve onayı ile paylaşılmaktadır.
- Öğrenci içerikli tüm paylaşımlarda velilerin izinleri alınmaktadır.
- Veli izni yanında öğrencinin de izni olmadan fotoğrafı çekilip kullanılmamaktadır.

KULLANICILAR

- ✓ Öğrenciler tarafından hazırlanacak olan bir video henüz hazırlanmadan önce, bununla ilgili görev alan öğrenciler, öğretmenlerinden izin almalıdır.
- ✓ Paylaşılan tüm öğrenci bazlı etkinliklerde, etkinlik öncesinde velilerin izinleri alınmalıdır.
- ✓ Video konferans, resmi ve onaylanmış siteler aracılığıyla yapılacaktır.
- ✓ Kullanıcılar, şahsi sosyal medya hesaplarında, okul öğrencileri ve çalışanlarının yer aldığı görselleri, okul yetkili mercileri tarafından onaylanmadan paylaşamazlar

İÇERİK

- ❖ Video konferans yapılırken, tüm kullanıcıların katılabileceği siteler üzerinden yapılacaktır.
- ❖ Video konferans yapılmadan önce diğer okullarla iletişim kurulmuş olması gerekmektedir.
- ❖ Okul öğrenci ve çalışanlarını ilgilendiren/içinde bulunduran tüm içerik, ancak kontrol ve onay süreçlerinden geçtikten sonra, paylaşıma açık hale gelecektir.

İNTERNETİN VE BİLİŞİM CİHAZLARININ GÜVENLİ KULLANIMI

- İnternet; bilgiye ulaşmakta en önemli araçlardan biri haline gelmişken, bunu okuldaki müfredat ile ilişkilendirerek doğru bilgiye en güvenli şekilde öğrencilerimizi ve öğretmenlerimizi ulaştırabiliyoruz.
- İnternet erişimlerimizi öğrencilerimizin yaş ve yeteneklerine göre entegre etmiş durumdayız.
- Tüm okulumuza ait bilişim cihazlarımızı kullanım politikamıza uygun şekilde, MEB güvenlik sertifikalarını yükleyerek güvenli hale getirmiş bulunuyoruz.
- Tüm çalışanlarımız, velilerimiz ve öğrencilerimiz etkili ve verimli çevrimiçi materyallerin kullanımı konusunda bilgilendirilmiştir.
- E-güvenlik ve siber zorbalık konuları belli derslerimizin yıllık planlarına dahil edilmiş olup, bu konularda yıl içinde öğrencilere bilgi aktarımı devam etmektedir.
- Çevrimiçi materyaller öğretme ve öğrenmenin önemli bir parçası olup müfredat içinde aktif olarak kullanılmaktadır.
- 6 Şubat güvenli internet günü okulumuzda kutlanmaktadır.

CEP TELEFONLARI VE KİŞİSEL CİHAZLARIN KULLANIMI

- ✓ Okulumuz ilkokulu olduğu için öğrencilerin okula cep telefonu getirmeleri yasaktır.
- ✓ Okulumuz öğrencileri, velilerini aramaları gerektiği durumlarda okula ait olan telefonları bir okul idarecisi gözetiminde kullanabilirler.
- ✓ Öğrencilerimiz eğitim amaçlı (web 2.0 araçlarının kullanımı vb) kişisel cihazlarını kullanmak için okul yönetiminden izin almalıdır.
- ✓ Velilerimiz okul saatleri içerisinde öğrencileriyle görüşme yapmamaları gerektiği konusunda bilgilendirilirler. Eğer zorunlu haller var ise okul yönetiminden izin alarak görüşme yapmaları sağlanmalıdır.
- ✓ 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.
- ✓ 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.

E-GÜVENLİK EĞİTİMİ

- ❖ Öğrenciler içine-güvenlik müfredatı ilgili derslerin yıllık planlarına eklenerek öğrenciler bu konularda bilgilendirilir.
- ❖ Tüm kullanıcıların internet kullanımları bilgi işlem birimi tarafından takip edilmektedir. Bu bilgi tüm kullanıcılara iletilmiştir.
- ❖ Öğrencilerimizin ihtiyaçları doğrultusunda çevrim içi güvenliği geliştirmek için rehberlik öğretmenleri akran eğitimi uygulamaktadır.
- ❖ Teknolojiyi olumlu kullanan öğrenciler ödüllendirilecektir.
- ❖ Çevirim içi güvenlik politikası tüm çalışanlarımıza resmi olarak duyurulacaktır.
- ❖ 6 Şubat güvenli internet günü okulumuzda kutlanmaktadır. Bu güne yönelik okul koridorları ve sınıflarda pano çalışmalarımız ve sosyal medya paylaşımlarımız olur.

ÇEVRİMİÇİ OLAYLAR VE KORUMA

- ➢ Okulumuzun tüm üyeleri çevirim içi riskler konusunda bilgilendirilecektir. Eğitimler yapılıp içerikler açıklanacaktır.
- ➢ Okulumuzda yasadışı içerik, güvenlik ihlali, siber zorbalık, cinsel içerikli mesajlaşma, çocuk istismarı, kişisel bilgi güvenliği gibi konularda bilgilendirme çalışmaları yapılmaktadır.
- ➢ 6 şubat güvenli internet günü kutlanmaktadır.
- ➢ Okulumuzda internet, bilgi teknolojileri ve ekipmanlarının yanlış kullanımı ile ilgili tüm şikayetler okul müdürüne bildirilecektir.

- Okulumuzun tüm üyeleri gizlilik ve güvenlik endişelerini ortadan kaldırmak için resmi okul kurallarına uygun şekilde davranmaları hususunda bilgilendirilir.
- Yaşanan olumsuzluklarda okul gerekli işlemleri yapmakla sorumludur.
- Sorunların çözümünde çalışanlar (öğretmen, idareci, personel vb),veliler ve öğrenciler okul ile birlikte hareket etmelidir.

TÜM ÇALIŞANLARIN SORUMLULUKLARI ŞUNLARDIR

- ✓ Çevrimiçi güvenlik politikalarının geliştirilmesine katkıda bulunmak.
- ✓ Okul sistemlerinin ve verilerin güvenliğinden sorumlu olmak.
- ✓ Yeni ve gelişmekte olan teknolojiler kullanıldığında iyi uygulamaları modellemek.
- ✓ Mümkün olduğunca müfredat ile çevrimiçi güvenlik eğitimini ilişkilendirmek.
- ✓ Olumlu öğrenme fırsatlarına vurgu yapmak.
- ✓ Bu alanda mesleki gelişim için kişisel sorumluluk almak.

ÇOCUKLARIN BAŞLICA SORUMLULUKLARI ŞUNLARDIR

- ❖ Çevrimiçi güvenlik politikalarının geliştirilmesine katkıda bulunmak.
- ❖ 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.
- ❖ Belli bir teknolojiyi kullanmanın kişisel risklerini değerlendirmek ve bu riskleri sınırlamak için güvenli ve sorumluluk sahibi davranmak.

EBEVEYNLERİN BAŞLICA SORUMLULUKLARI ŞUNLARDIR

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