



## **EMİRGAZİ MEHMET AKİF ERSOY İLKOKULU**

### **E-GÜVENLİK OKUL POLİTİKASI ve KURALLARI**

## **EMİRGAZİ MEHMET AKİF ERSOY PRIMARY SCHOOL**

### **E-SECURITY (eSafety) SCHOOL POLICY and RULES**

Gençler ve teknoloji, günümüz dünyasında çoğu kez ayrılamaz. Web'in kullanımı artarken, güvenli kullanımıyla da ilgilidir. Güvenli bir ortam sağlamak için, risklerin çeşitlerini ve sıklığını ve bunları azaltmak veya daha da iyisi ortadan kaldırmak için çözümleri anlamamız gerekir. Gençler çevrimiçi ortamda karşılaşılan riskler konusunda daha genç kullanıcılar için daha güvenli bir internet yaratmanın yolları ile ilgili önemli miktarda araştırma yapılmıştır. Çevrimiçi gençlerin karşılaştığı risklerden biri de siber zorbalık veya çevrimiçi mağduriyettir: yani elektronik iletişim şekillerini kullanan zorbalık veya taciz. Siber zorbalığın bazı örnekleri açıkça tanımlanabilirken diğerleri daha azdır. Siber kelimenin mağdurunu korkutmak için kullandığı dil ve taktiklerin cezai bir suç olduğunun açık işareti olduğu durumlarda olabilir, bazı durumlarda ise yalnızca bir şahsın kötü davranışlarından kaynaklanır. Siber zorbalık, genellikle eylemin tekrarını gerektirir. Siber zorbalığı yaygınlaştırma konusunda, özellikle geleneksel zorbalığa kıyasla açık bir anlaşma eksikliği var ve bu, yaygınlığı hakkındaki istatistikleri etkiliyor. İnternetteki siber zorbalığa hitap etmenin bir yolu, okul zorbalığı ve siber zorbalık arasındaki bağlantıyı kullanmaktır. Okul zorbalığına, gençlerin sahip oldukları ve birbirlerine karşı olan ilişkileri ve tutumları geliştirmeye çalışan girişimler denir. Bu tür girişimleri, çevrimdışı zorbalığa karşı koymak için potansiyel olarak etkili önleme tedbirleri olarak düşünülmemekte ve çevrimiçi zorbalığa karşı koymada da yararlı olabilirler. Gençler ve yetişkinler genellikle çevrimiçi mağduriyet konusunda farklı yorumlara sahiptir. Yetişkinler bazı eylemleri bir şekilde tedavi etme eğilimi gösterirken, gençler aynı örnekleri akranları arasında normal bir etkinlik olarak açıklayabilir, ancak bunlar çevrimdışı bir sorunla başlar. Okullar, okul çapında bir zorbalık önleme programının oluşturulmasını kolaylaştıracak politikalar oluşturur ve bu programlar tipik olarak etkinliklerinin periyodik değerlendirmelerini içerir. Başarılı ve etkili programlar, bireysel öğrencilerden ve sınıflardan, eğitimcileri ve öğrencileri birleştiren zorbalık karşıtı takımlara kadar, okulda her seviyede zorbalık karşıtı stratejileri teşvik etmek için çalışır. Ağır internet kullanıcıları uygunsuz içerikle çevrimiçi karşılaşabilir; Gençler genellikle cinsel taciz veya cinsel içeriğe online olarak maruz kalma ile karşı karşıya kalabilir. World Wide WB'deki sınırsız içerik, olgunlaşmamış gençleri istenmeyen

cinsel içeriğin ve bilginin geniş bir koleksiyonuna götürebilir. Örnekler, cinsel ilişki talepleri, cinsel konuşmalar, cinsel fotoğraflar gönderme veya talep etme veya istenmeyen cinsel bilgilerin ifşa edilmesini içerir. Ayrıca, istenmeyen pop-up'lar vasıtasıyla cinsel olmayan içerik için web'de gezinirken, gençler bazen müstehcen içerik veya cinsel imgelem / videolarla karşı karşıya kalırlar. E-posta dolandırıcılıkları alabilirler. İstenmeyen cinsel buluşmalarla uğraşmak için en yaygın önerilen strateji, gençleri bu tür sağlayıcıları engellemeye teşvik etmek veya onlara yardım etmek veya sorun yaşadıkları çevrimiçi forumdan ayrılmaktır. Çoğu genç, utanç yüzünden çevrimiçi olarak karşılaştıklarında yetişkinleri dâhil etmeme eğiliminde oldukları için, ebeveynlerin ve eğitimcilerin, gençlerin zorluklarla karşılaşabileceğini belirtmek için dikkat etmeleri gereken işaretlerden haberdar edilmesi gerekir. Bu nedenle, kurslar ve bilgilendirici görüşmeler genellikle okullarda veya yerel konseyler tarafından organize edilirken, diğer etkin yöntemler filtreleme ve güvenlik duvarı teknolojilerini içerir. Buna ek olarak, internet erişimi sağlayan 2 şirketlerin kullanıcıları için daha güvenli çevrimiçi ortamlar sağlamaları, dolayısıyla çevrimiçi riskleri ele almanın bir başka yolunu teşvik etmeleri önerilir. Gençlerin daha proaktif olarak çevrimiçi mahremiyetlerini korumaları durumunda, internetin oluşturduğu risklerin birçoğu azaltılabilir. Kişisel bilgilerin çevrimiçi olarak açığa çıkmasına daha az istekli olacak şekilde eğitilmeleri ve gizliliklerini nasıl yöneteceklerini bilmeleri gerekir; Bu tür eğitim, özellikle genç yaştan itibaren okullarda önemlidir. Ebeveynler ve çocukları arasındaki nesil boşluğu nedeniyle, birbirlerine güven duymalarını engelleyebilecek ve dolayısıyla çevrimiçi riskin etkili bir şekilde kontrol altına alınmasına neden olabilecek bir yanlış anlaşılma olasılığı bulunmaktadır. Bu nedenle, gençlerle yetişkinler arasındaki iletişim teşvik edilmelidir; siber güvenlikle ilgili diyaloga girmek, boşluğu hafifletmeye ve güvenlik tedbirlerini geliştirmeye yardımcı olabilir. Bu tür diyaloglar aynı zamanda gençleri ebeveynlerini çevrimiçi olan kaynaklar ve web siteleri konusunda eğitmeye teşvik edebilir, Yarın dünyanın liderleri arasında internet güvenlik tedbirlerini tartışmak çok önemlidir. Web'in sağladığı yararlar modern kültürümüzün bir parçasıdır ve birçok teknolojik ilerlememizin gençlerin kendilerinin güvenliği konusunda geri tepmesine izin vermemeliyiz.

### **AMAÇ:**

- Mehmet Akif Ersoy İlkokulu Müdürlüğü, e-güvenlik çalışmaları ile internet, akıllı tahta, 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 mesleki gelişim için sorumluluk almak.
- Okulu ve içerisindekileri korumak için e-güvenlik konusunda sorumluluk almak.
- Teknolojiyi güvenli ve sorumlu kullanmak.
- Zarar görülmesi durumunda tehlikeyi gözlemleyip ilgili birimlere iletmek.

### **OKUL WEB SİTESİ:**

- Mehmet Akif Ersoy İlkokulu Müdürlüğü olarak web sitemizde okulumuzun adres, telefon, fax ve e posta adres bilgileri bulunmaktadır.
- Sitemizde yayınlanan tüm içerikler okul müdürünün onayından geçtikten sonra bilgi işlem birimi tarafından siteye konulmaktadır.
- Okulumuzun web sitesi bilgi işlem birimimizin sorumluluğunda olup güçlü güvenlik önlemleri alınmış durumdadır.
- Öğrenci çalışmaları, velilerinin izinleriyle yayımlanmaktadır.

### **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.
- Okul idaresi tarafından görevli kılınanlar haricindeki kişiler tarafından ve öğrenci velilerinin bilmek istedikleri etkinlik ve programlar dışındaki zamanlarda, okul ve okul bahçesi sınırları içerisinde fotoğraf ve video çekimi yapılamaz.
- Okul idaresi tarafından görevlendirilen kişilerin çektiği fotoğraf ve videolar ancak Okulun resmi web adresinde ve sanal ortamlarında, ilgili öğrenci velisinin talep ve yazılı onayı ile yayınlanabilir
- Okul görevlileri tarafından yayınlanan resim ve videolarda öğrencilerin kişisel bilgilerine kesinlikle yer verilmez.

### **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, paylaşımına 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, gerekli filtrelemeleri yaparak güvenli hale getirmiş durumdayız.
- Tüm çalışanlarımız, velilerimiz ve öğrencilerimiz etkili ve verimli çevrimiçi materyallerin kullanımını 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 öğretim ve öğrenmenin önemli bir parçası olup müfredat içinde aktif olarak kullanılmaktadır.
- Güvenli internet günü çeşitli etkinliklerle okulumuzda kutlanmaktadır.

### **GÜVENLİK EĞİTİMİ:**

- Öğrenciler için e-güvenlik müfredatı ilgili derslerin yıllık planlarına eklenerek öğrenciler bu konularda bilgilendirilir.
- Öğrencilerimizin ihtiyaçları doğrultusunda çevrimiçi güvenliği geliştirmek için sınıf rehber öğretmenleri akran eğitimi uygulamaktadır.
- Teknolojiyi olumlu kullanan öğrenciler ödüllendirilecektir.
- Çevrimiçi güvenlik politikası tüm çalışanlarımıza resmi olarak duyurulacaktır.
- 6 Şubat güvenli internet günü okulumuzda kutlanmaktadır. Bu güne yönelik okul koridorları ve sınıflarda pano çalışmaları ve sosyal medya paylaşımları yapılacaktır.

## **CEP TELEFONLARI VE KİŞİSEL CİHAZLARIN KULLANIMI:**

- Okul saatleri içinde öğrencilerimizin kişisel cep telefonu kullanımı yasaktır.
- 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 almaktadır; fakat sorumluluk kişiye aittir.
- Okulumuz öğrencileri, velilerini aramaları gerektiği durumlarda okula ait olan telefonları bir okul idarecisi gözetiminde kullanabilirler.
- Öğrencilerimiz eğitim amaçlı (web 2 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.
- 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.

## **ÇEVİRİMİÇİ OLAYLAR VE KORUMA:**

- Okulumuzun tüm üyeleri çevrimiçi riskler konusunda bilgilendirilecektir.
- Okulumuzda yasadışı içerik, güvenlik ihlali, siber zorbalık, cinsel içerikli mesajlaşma, çocuk istismarı, kişisel bilgi güvenliği gibi konularda bilgilendirme çalışmaları yapılmaktadır.
- Güvenli internet gününde çeşitli etkinlikler düzenlenerek farkındalık oluşturulmaya çalışılmaktadır.
- 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.

## **OKUL PERSONELİ**

EuropeanSchoolnet (www.eun.org) tarafından her yıl yapılan eğitimlere katılmaktadırlar Okulumuz personeli BIT koordinatörü tarafından eğitim almaktadırlar. Yine eTwinning mesleki gelişim portalından çevrimiçi ve online mesleki gelişim etkinliklerine katılmışlardır. 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 çeşitli şekillerde sağlanacaktır. Çalışanların hepsi, çevrimiçi davranışlarının okuldaki rolü ve itibarını etkileyebileceğinin farkına varacaktır. Mesleği veya kurumu tehlikeli durumuna düşürdüğü veya mesleki yeteneklerine güvenini kaybetmiş bir şeyin bulunduğu düşünülürse, hukuk, 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 olacaklardır. Okul çalışanların öğrencilerin yaşlarına ve yeteneklerine göre kullanması gereken yararlı çevrimiçi araçları kontrol etmelidir. Çocukların internetin ve dijital teknolojinin güvenilir ve sorumlu kullanıcıları olabilmesi için ana-babanın / bakıcıların oynayacakları önemli bir role sahip olduklarını kabul eder. Ebeveynlerin dikkatleri, bültenler, mektuplar, okul izahname ve okul web sitesinde okulun çevrimiçi güvenlik (e-Güvenlik) politikasına ve beklentilerine yönelecektir. Evde ve okulda ebeveynlerle çevrimiçi güvenlik konusundaki işbirlikçi, yaklaşımı teşvik edilecektir. Evde güvenli İnternet kullanımı için gösteriler ve öneriler içeren ebeveyn eğitimleri sunma veya diğer iyi katılan etkinliklerde çevrimiçi güvenliğin vurgulanmasını içerebilir. Ebeveyn eğitimleri, birlikte vakit geçirme ve spor günleri, gibi sosyal etkinlikler düzenleyeceklerdir. 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. Ebeveynler, çevrimiçi olarak çocukları için rol modeli olumlu davranışlar teşvik edilecektir

## **GÜVENLİ İNTERNET KULLANIMI KAPSAMINDA YAPILAN ÇALIŞMALAR**

Çağımızın en önemli iletişim araçlarından biri olan internetin, bilinçli kullanımı zararlı içeriklerinden korunma, siber zorbalık ve istismar önemli bir hal almıştır. Bu bağlamda çocuklarımızın

internetin zararlı içeriklerinden ve istismarlardan korunması için okulumuzda yapılan çalışmalar aşağıda listelenmiştir:

1. Öğrencileri bilinçli internet kullanımına yönelik bilgilendirme amacıyla hazırlanmış <http://www.eba.gov.tr> adresinde yer alan "Teknolojinin Doğru Kullanımı / Bilinçli İnternet" programları kapsamında sınıf rehber öğretmenleri tarafından eğitimler verilmiştir.
2. Okullarda internet ağını ve ağ üzerinde yapılan paylaşımların güvenliği, gizliliği ve olası tehditlere karşı bir önlem olarak geliştirilmiş MEB Sertifikası tablet, akıllı tahtalar, bilgisayar ve cihazlara yüklenmiştir.
3. Evde internet kullanımı konusunda "Güvenli Çocuk" ve "Güvenli Aile" paketlerinin kullanımı konusunda teşvik edici çalışmalar yapılmıştır.
4. Sosyal ağ siteleri kullanımı sırasında gizlilik içeren bilgilerin (doğum tarihleri, telefon numaraları, adresler vb.) paylaşılmaması konusunda bilgilendirme çalışmaları yapılmıştır.
5. Kişisel verilerin korunması kapsamında; okul internet sitesinde kişiyi tam olarak belirlenebilir kılan (T.C. Kimlik No, anne-baba adı, iletişim ve ikametgâh bilgileri vb.) bilgilerin paylaşılmamasına özen gösterilmektedir.
6. Okul internet sitesinde, öğrenciler için eğitici niteliği olmayan, pedagojik açıdan sakıncalı içerik, bağlantı ve medya (oyun, video, uygulama ve benzeri) yayımlanmamasına hassasiyet gösterilmektedir.
7. Bilgi Teknolojileri ve İletişim Kurumu tarafından hazırlanan afişler okul panolarında sergilenmiştir.
8. Millî Eğitim Bakanlığı Bilgi ve Sistem Güvenliği Yönergesi kapsamında kurum ağına sadece Bakanlık hattı kullanılmakta; haricindeki internet hatlarının (ADSL, VDSL 3G. Wireless vb.) kullanılmasına müsaade edilmemektedir.

