

E Güvenlik Politikası

e-Güvenlik (e-Safety) POLİTİKASI VE AMAÇLARI

Dijital çağ olarak adlandırılan günümüzde; teknolojinin hızla gelişmesiyle birlikte her okulun Okul Güvenlik Politikasının olması kaçınılmaz olmuştur. Çünkü paydaşlar günümüzde okul binasından çok çeşitli şekillerde internete erişebilmektedirler.

Dijital teknoloji artık günlük hayatımızın bir parçası olmuştur. Çocuklarımızın dijital teknolojiler aracılığıyla mevcut olan fırsatlardan en iyi nasıl faydalanabileceklerini bilmeleri için, öncelikle nasıl kullanacaklarını öğrenmeleri gerekmektedir. Bunun mümkün olan en güvenli şekilde ve ortamda yapılmasını sağlamak için, açık ve özlü bir Güvenli İnternet Okul Politikasına sahip bir okuluz.

A. ÖZETLE E-GÜVENLİK (E-SAFETY) POLİTİKAMIZ:

- 1- Okulumuzda ders anlatımı yapılan her alanda etkileşimli tahta ve güvenli, içerik filtresi uygulanmış erişim ağı vardır. Ders anlatımlarında eba eğitim portalı ve diğer güvenli eğitim içeriklerinden sıklıkla yararlanılmaktadır.
- 2- Okulumuzun internet sitesi ve sosyal ağları bulunmaktadır.
- 3- Bu ağların üzerinde yayınlanan veriler oluşturulan komisyon tarafından kontrol edilerek paylaşılmaktadır.
- 4- Etkileşimli tahtalar öğretmene özel oluşturulan şifre ya da flash kilit anahtarı ile öğretmen kontrolünde kullanılmaktadır.
- 5- Öğrencilerimizin okul içerisinde çep telefonu kullanımlarına izin verilmemektedir.
- 6- Okulumuzda öğretmenlerimizin cep telefonları ders esnasında kapalı konumda tutulmaktadır.
- 7- Rehberlik servisi tarafından, her sınıf düzeyinde düzenli olarak, Siber Zorbalık gibi konularda seminerler verilmektedir.
- 8- Okulumuzun öğretmenleri Milli Eğitim Bakanlığı tarafından verilen İnternet Güvenliği, ve derslerde kullanacakları 2.0 Web eğitimlerini uzaktan ve yüz yüze eğitimler olarak almışlardır.
- 9- Okulumuzun internet sitesinde e-güvenlik konusunda, güvenliweb.org.tr sitesi ve buradan alıntılanan öğrenci ve velilere yönelik videolar ve afişler yer alan linkler yer almaktadır. Okul paydaşlarımız istedikleri zaman konu ile ilgili bilgileri alabilmektedirler.
- 10- Okulumuzda Dijital vatandaş olma konusunda paydaşlarımızı bilinçlendirme çalışmaları yapılmaktadır.

B. OKULUMUZDA E-GÜVENLİK POLİTİKASININ AMACI

- 1- Okulumuzun tüm üyelerini çevrimiçi olarak korumak ve güvenliğini sağlamak.
- 2- Teknolojinin potansiyel riskleri ve yararları konusunda öğretmenler, öğrenciler ve çalışanlar için farkındalık yaratmak.
- 3- Tüm personelin güvenli ve sorumlu bir şekilde çalışmasını sağlamak.
- 4- Okuldaki tüm üyeler tarafından bilinen çevrimiçi güvenlik endişelerine yanıt verirken açıkça kullanılacak prosedürleri tanımlamak.
- 5- Sonuç olarak ana hedefimiz, internet erişimi için bu güvenlik politikasının geçerli olmasıdır.

TÜM ÇALIŞANLARIN KİLİT SORUMLULUKLARI ŞUNLARDIR:

- 1- Çevrimiçi güvenlik politikalarının geliştirilmesine katkıda bulunmak.
- 2- Okul sistemlerinin ve verilerin güvenliğinden sorumlu olmak.
- 3- Bir dizi farklı çevrimiçi güvenlik konusundaki farkındalığa sahip olmak ve onların bakımında çocuklarla nasıl ilişkili olabileceklerini bilmek.
- 4- Yeni ve gelişmekte olan teknolojiler kullanıldığında iyi uygulamaları modelleme.
- 5- Müfredat ile çevrimiçi güvenlik eğitimini ilişkilendirme.
- 6- Bu alanda mesleki gelişim için kişisel sorumluluk almak.

ÇOCUKLARIN VE GENÇLERİN BAŞLICA SORUMLULUKLARI ŞUNLARDIR:

- 1- Çevrimiçi güvenlik politikalarının geliştirilmesine katkıda bulunmak.
- 2- Çevrim içi ve çevrimdışı başkalarının hislerine ve haklarına saygı duymak.
- 3- İşler ters giderse, güvenilir bir yetişkinden yardım istemek ve çevrimiçi güvenlik sorunlarıyla karşılaşan diğer kişileri desteklemek.
- 4- Bireysel yaşlarına, yeteneklerine ve zayıf yönlerine uygun bir seviyede:
 - Kendilerini ve başkalarını 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 BAŞLICA SORUMLULUKLARI ŞUNLARDIR:

- 1- Okul Politikalarını okumak, çocuklarını bu politikaya bağlı kalmaya teşvik etmek ve uygun olduğunca kendilerinin de bağlı kalmasını sağlamak.
- 2-Çocuklarıyla çevrimiçi güvenlik konularını tartışmak, okulun çevrimiçi güvenlik yaklaşımlarını desteklemek ve evde uygun güvenli çevrimiçi davranışları pekiştirmek.
- 3- Teknoloji ve sosyal medyanın güvenli ve uygun kullanımını modellemek.
- 4- Davranışlarında, çocuğun çevrimiçi olarak zarar görme tehlikesi altında olduğunu gösteren değişiklikleri belirlemek.
- 5- Okul veya diğer uygun kurumlardan, kendileri veya çocukları çevrimiçi problem veya sorunlarla karşılaşarsa yardım veya destek istemek.
- 6- Okulun çevrimiçi güvenlik politikalarının oluşturulmasına katkıda bulunmak.
- 7- Öğrenme platformları ve diğer ağ kaynakları gibi okul sistemlerini güvenli ve uygun bir şekilde kullanmak.
- 8- 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:

- 1- Web sitesinde iletişim bilgileri okul adresi, e-posta ve telefon numarası olacaktır. Personel veya öğrencilerin kişisel bilgileri yayınlanmayacaktır.
- 2- Okul Müdürü ve yayın kurulu, yayınlanan çevrimiçi içerik için genel yayın sorumluluğunu alacak ve bilgilerin doğru ve uygun olmasını sağlayacaktır.
- 3- Web sitesi, erişilebilirlik fikri mülkiyet haklarına saygı, gizlilik politikaları ve telif hakkı da dahil olmak üzere okulun yayın yönergelerine uyacaktır.
- 4- Spam maillerden korunmak için e-posta adresleri çevrimiçi olarak dikkatli bir şekilde yayınlanacaktır.
- 5- Öğrenci çalışmaları ebeveynlerinin izniyle yayınlanacaktır.
- 6- Okul web sitesinin yönetici hesabı, uygun bir şekilde güçlü şifreyle şifrelenerek korunacaktır.

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

8- Okul, çevrimiçi paylaşılan tüm resimlerin ve videoların okul politikasına uygun şekilde kullanılmasını sağlayacaktır.

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

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

Video Konferans Kuralları

1- Öğrenciler, bir video konferans araması veya mesajı hazırlamadan veya cevaplamadan önce bir öğretmenin izin isteyecektir.

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

3- Velilerin rızası, çocuklar video konferans faaliyetlerine katılmadan önce alınacaktır.

4- Video konferans, sağlam bir risk değerlendirmesini takiben, resmi ve onaylanmış iletişim kanalları vasıtasıyla gerçekleşecektir.

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

6- Eğitimsel video konferans servisleri için özel oturum açma ve şifre bilgileri yalnızca personellere verilecek ve gizli tutulacak.

Kişisel Cihazların ve Cep Telefonlarının Kullanımı

1- 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.

2- 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.

3- Müjgan Çetin Okulları, mobil teknolojilerle yapılan kişisel iletişimin, çocuklar, personel ve anne-babalar için gündelik yaşamın kabul edilen bir parçası olduğunun farkındadır; ancak, bu tür teknolojilerin okulda güvenli ve uygun bir şekilde kullanılmasını gerektirir.

Öğrencilerin Kişisel Cihazlarını Ve Cep Telefonlarını Kullanımı

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

2- Bilişim araçlarını, okul yönetimi ile öğretmenin bilgisi ve izni dışında konuşma yaparak, ses ve görüntü alarak, 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.

3- Öğrenciler ders başlamadan önce telefonlarını okul yönetimi tarafından yaptırılan telefon kutularına koymakla yükümlüdür. Cep telefonunun amacı dışında kullanımı ihlali olduğunda, 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 edilinceye kadar güvenli bir yerde tutulur.

4- Velisi dışında telefon kimseye teslim edilmez.

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

6- 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.

7-Çocukların cep telefonlarını veya kişisel cihazlarını eğitim etkinliğinde kullanımı, okul idaresi tarafından onaylandığında gerçekleştirilecektir.

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

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

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

11- Öğrencilere, cep telefonlarının ve kişisel cihazların güvenli ve uygun bir şekilde kullanımı öğretilecek ve sınırların ve sonuçların farkına varılacaktır.

12- 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.

Ziyaretçiler Kişisel Cihazların Ve Cep Telefonlarının Kullanılması

1- Ebeveynler ve ziyaretçiler, okulun politikasına uygun olarak cep telefonlarını ve kişisel cihazları kullanmalıdır.

2- Fotoğraflar veya videolar çekmek için ziyaretçiler ve ebeveynler tarafından cep telefonlarının veya kişisel cihazların kullanılması, okul politikasına uygun olarak gerçekleştirilmelidir.

3- Okul, ziyaretçilere kullanım beklentilerini bildirmek için uygun tabela ve bilgileri sağlayacak ve sunacaktır.

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

Öğrencilerin Katılımı Ve Eğitimi

1- 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.

2- Güvenli ve sorumlu kullanım ile ilgili eğitim internet erişiminden önce yapılacaktır.

3- Müfredat geliştirme ve uygulama da dahil olmak üzere okul çevrimiçi güvenlik politikaları ve uygulamaları yazarken ve geliştirirken öğrenci katkıları aranacaktır.

4- Öğrenciler okul Politikasını, yaşlarına ve yeteneklerine uygun bir şekilde okumak ve anlamak için desteklenecektir.

5- Tüm kullanıcılara ağ ve internet kullanımının izleneceği bildirilecektir.

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

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

8- Okul, öğrencilerin teknolojiyi olumlu şekilde kullandıklarını ödüllendirecektir.

9- Okul, öğrencilerin ihtiyaçlarına uygun olarak çevrimiçi güvenliği geliştirmek için akran eğitimini uygulayacaktır.

Personelin Katılımı ve Eğitimi

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

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

3- 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.

4- 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.

