e- Güvenlik

**Kabul Edilebilir Kullanım Politikası (AUP) Bilgilendirme Metni**

Kabul Edilebilir Kullanım Politikamız (AUP); yöneticiler, öğretmenler, veliler, tüm personel ve öğrenciler için hazırlanmış olup, internet erişimi ve bilgi iletişim cihazlarının kullanımı için geçerlidir.

* 1. **AMAÇ**:
1. Kurum personelinin, öğrenci ve velilerimizin sistem, bilgi ve varlıkların gizlilik, bütünlük ve erişilebilirlik özelliğini garantilemek için yapması ve uyması gereken kuralları kendilerine iletmek.
2. AUP politikamız ile okulumuz ‘un tüm üyelerini çevrimiçi olarak korumak ve güvenliğini sağlamak. Teknolojinin potansiyel riskleri ve yararları konusunda farkındalık yaratmak.
3. Okulumuzda kullanılacak e-güvenlik politikası prosedürlerini tanımlamak.
4. Kurum personeli, öğrenci ve velilerimizin güvenli ve sorumlu teknoloji kullanımı konusunda uyması gereken kuralları rolleri ve davranışları tanımlamak.

**2.1. OKUL TOPLULUĞUMUZ İÇİN ANA RİSK ALANLARI:**

1. Çevrimiçi uygunsuz içeriğe maruz kalma,
2. Zararlı siteler
3. Facebook, Instagram, YouTube, WhatsApp gibi uygulamalarda yaş kısıtlamalarını göz ardı etmek.
4. Veri ihlali
5. Bilgi doğrulama
6. Çevrimiçi oyunlarda yaş derecelendirmelerini göz ardı etmek (genellikle sözel şiddete maruz kalma, bağımlılık, uygulama içi satın alımlar).

**3.1. BAŞLICA SORUMLULUKLARIMIZ:**

**İdare;**

1. e-Güvenlik sağlanması için genel sorumluluk almak.
2. GDPR uyumlu veri ve veri güvenliği için sorumluluk almak.
3. Okulda, mevcut yasal gerekliliklere uygun onaylanmış, filtrelenmiş bir internet hizmeti kullanılmasını temin etmek.
4. Personelin e-güvenlik rollerini yerine getirmesini ve diğer meslektaşlarını uygun şekilde eğitmek için gerekli eğitimi almasını sağlamak.
5. Ciddi bir e-güvenlik olayı durumunda izlenecek eylem planını takip etmek.
6. e-Güvenlik Komisyonu'ndan e-güvenlik hakkında düzenli izleme raporları almak.
7. e-Güvenlik prosedürlerini yürüten personeli denetlemek ve desteklemek.
8. Veliler ve öğrencilerle dijital iletişim kanalları üzerinden yapılan iletişimin politikalarımıza uygunluğunu takip etmek.

 **e-Güvenlik Komisyonu;**

* 1. e-Güvenlik sorunlarının izlenmesi sorumluluğunu alıp okulun e-Güvenlik politikalarının / dokümanların oluşturulmasında ve güncellenmesinde öncü olmak.
	2. Okul topluluğunda e-güvenliğe yönelik farkındalık oluşması ve olumlu davranışlar gelişmesini teşvik etmek.
	3. Müfredat kapsamındaki e-güvenlik eğitimine katkı sağlamak.
	4. Okulda e-Güvenlik ile ilgili paydaşların koordinasyonunu sağlamak.
	5. Bakanlık tarafından e-Güvenlik ile ilgili gönderilen yazıların eyleme geçirilmesini sağlamak.
	6. Mevcut sorunları tartışmak, vaka kayıtlarını gözden geçirmek ve filtreleme / değişiklik kontrol günlüklerini gözden geçirmek için toplantılar düzenlemek.
	7. Tüm personelin bir e-Güvenlik olayı durumunda takip edilmesi gereken prosedürlerden haberdar olmasını sağlamak.
	8. e-Güvenlik olay kaydının güncel tutulmasını sağlamak ve idareye bildirmek.
	9. Yerel Otorite ve ilgili kurumlar ile bağlantı kurarak e-Güvenlik sorunları ve mevzuatını takip etmek.

**Öğretmenler ve Personeller;**

* 1. Çevrimiçi güvenlik politikalarının geliştirilmesine katkıda bulunmak.
	2. Kabul Edilebilir Kullanım Politikalarını okumak ve onlara bağlı kalmak.
	3. Okul sistemlerinin ve verilerin güvenliğinden sorumlu olmak.
	4. Çevrimiçi güvenlik konusunda farkındalığa sahip olmak ve öğrencileri de bu konuda bilinçlendirmek.
	5. Yeni ve gelişmekte olan teknolojiler kullanıldığında iyi uygulamaları modellemek.
	6. Mümkün olduğunca müfredat ile çevrimiçi güvenlik eğitimini ilişkilendirmek.
	7. Çevrimiçi güvenlik konularını tüm derslerin müfredatlarıyla ilişkilendirerek yaygınlaştırmak.
	8. Okul koruma politikalarını ve prosedürlerini takip ederek e-güvenlik açısından endişe duyan bireyleri belirleyerek, uygun önlemleri almak.
	9. Olumlu öğrenme fırsatlarına vurgu yapmak.
	10. e- Güvenlik alanında mesleki gelişim için kişisel sorumluluk almak.
	11. Herhangi bir şüpheli ve/veya yanlış kullanımı e-Güvenlik Komisyonu üyelerine bildirmek.
	12. Öğrencilerle kuracağı dijital iletişimlerin profesyonel düzeyde ve okul yönetimince sağlanan/takip edilen uygulamalar aracılığıyla yapılmasını sağlamak.
	13. Teknolojinin güvenli kullanımı konusunda örnek davranışlar sergileyerek, özellikle öğrenciler başta olmak üzere çevresindeki insanları güvenli teknoloji kullanımına teşvik etmek.

**Öğrenciler;**

* 1. Çevrimiçi güvenlik politikalarının geliştirilmesine katkıda bulunmak.
	2. Okulun Kabul Edilebilir Kullanım Politikalarını okumak ve onlara bağlı kalmak.
	3. Çevrim içi ve çevrimdışı başkalarının hislerine ve haklarına saygı duymak.
	4. İşler ters giderse, güvenilir bir yetişkinden yardım istemek ve çevrimiçi güvenlik sorunlarıyla karşılaşan diğer kişileri desteklemek.
	5. Başkalarının kişisel verilerini izinsiz paylaşmamak.
	6. Kendilerini ve başkalarını çevrimiçi olarak korumak için sorumluluk almak.
	7. Yeni ve gelişmekte olan teknolojilerin getirdiği fırsatlar ve riskleri araştırarak, okul topluluğunu da bilgilendirmek.
	8. Okul dışında dijital teknolojileri kullanırken e-Güvenlik politikamıza uygun davranışları benimsemenin önemini anlamak ve anlatmak.
	9. Cep telefonlarının, dijital kameraların ve taşınabilir cihazların kullanımı ile ilgili okul politikasına uygun davranmak.

 **Veliler;**

* 1. e-Güvenliği teşvik etmede okulu desteklemek ve öğrencilerin interneti kullanımı ve okulun öğrenci fotoğraf ve video görüntülerini kullanmasını içeren Kabul Edilebilir Kullanım Politikası Bilgilendirme Sözleşmesi'ni kabul etmek.
	2. Okul Kabul Edilebilir Kullanım Politikalarını okumak, çocuklarını bu politikaya bağlı kalmaya teşvik etmek ve uygun olduğunca kendilerinin de bağlı kalmasını sağlamak.
	3. Çocuklarıyla çevrimiçi güvenlik konularını tartışmak, okulun çevrimiçi güvenlik yaklaşımlarını desteklemek ve evde uygun güvenli çevrimiçi davranışları pekiştirmek.
	4. Teknoloji ve sosyal medyanın güvenli ve uygun kullanımını modellemek.
	5. Davranışlarında, çocuğun çevrimiçi olarak zarar görme tehlikesi altında olduğunu gösteren değişiklikleri belirlemek.
	6. Okul veya diğer uygun kurumlardan, kendileri veya çocukları çevrimiçi problem veya sorunlarla karşılaşırsa yardım veya destek istemek.
	7. Okulun çevrimiçi güvenlik politikalarının oluşturulmasına katkıda bulunmak.
	8. Öğrenme platformları ve diğer ağ kaynakları gibi okul sistemlerini güvenli ve uygun bir şekilde kullanmak.
	9. Yeni ve gelişmekte olan teknolojilerin getirdiği fırsatlar ve risklerle ilgili olarak kendi bilinci ve öğrenimlerinden sorumlu olmak.

# 4.1.   e-GÜVENLİK EĞİTİMİ:

* 1. Derslerin yıllık planlarına e-güvenlik konuları eklenerek öğrenciler bu konularda bilgilendirilir.
	2. Öğrencilerimizin ihtiyaçları doğrultusunda çevirim içi güvenliği geliştirmek için rehberlik öğretmenleri akran eğitimi uygulamaktadır.
	3. Teknolojiyi olumlu kullanan öğrenciler ödüllendirilecektir.
	4. Çevirim içi güvenlik politikası tüm çalışanlarımıza resmi olarak duyurulacaktır.
	5. Şubat ayında güvenli internet günü okulumuzda kutlanmaktadır. Bugüne yönelik okul koridorları ve sınıflarda pano çalışmalarımız ve sosyal medya paylaşımlarımız ve eğitimlerimiz olur.
	6. Okulumuzda internet, bilgi teknolojileri ve ekipmanlarının yanlış kullanımı ile ilgili tüm şikâyetler okul müdürüne bildirilecektir.
	7. Okulumuzun tüm üyelerinin gizlilik ve güvenlik endişelerini ortadan kaldırabilmek için; okul topluluğumuz resmi okul kurallarına uygun şekilde davranmaları hususunda bilgilendirilir.
	8. Yaşanan olumsuzluklarda okul gerekli işlemleri yapmakla sorumludur.
	9. Sorunların çözümünde çalışanlar (öğretmen, idareci, personel vb), veliler ve öğrenciler okul ile birlikte hareket etmelidir.

# 5.1. CEP TELEFONU KULLANIMI:

* 1. Sene başı öğretmenler kurulu toplantısında gündem maddesi olarak cep telefonu kullanımı görüşülmüştür. Öğrencilerin cep telefonlarını okula getirebileceklerine, fakat sabah okula geldiklerinde telefonların sınıf başkanlarınca toplanıp okul idaresine teslim edilmesine, toplanan telefonların idarece temin edilen kilitli dolaplarda saklanılmasına, okul çıkışında tekrar öğrencilere teslim edilmesine, öğrencilerin okulda telefon kullanmamalarına karar verilmiştir.
	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 bulundurmak kesinlikle yasaktır.
	3. Öğrencilere, kişisel cihazların ve cep telefonlarının güvenli ve uygun kullanımı konusunda eğitim verilecektir.
	4. Kabul Edilebilir Kullanım Politikasında, dijital teknolojilerin sınıfta nasıl kullanılabileceği ve kullanılamayacağına ilişkin tedbirler alınmıştır.
	5. Bir öğrenci ebeveynlerini arama gereği duyduğunda, okul idaresi veya şube rehber öğretmenine bildirecektir.
	6. Ebeveynlere okulun cep telefonu politikasıyla, bu önlemlerin neden alındığını ve politikanın ihlalinin ne gibi olası sonuçlar ortaya çıkarabileceğine ilişkin bilgi verilir.
	7. Amacı dışında kullanılan, cep telefonuna el konulması durumunda, telefonda özel verilerin korunmasını sağlamak için, okul İdaresine vermeden önce telefon kapatılmalıdır. Cep telefonu sahibine verilene kadar güvenli bir yerde tutulmalıdır.

**Ziyaretçilerin kişisel cihaz ve cep telefonu kullanması;**

* 1. Okulumuzda ziyaretçilerin fotoğraf/video kaydı almasına izin verilmemektedir.
	2. Ziyaretçiler kişisel cihazlarını okul politikamıza uygun kullanmakla yükümlüdür.
	3. İdare ziyaretçilere kullanım beklentilerini bildirmek için uygun tabela ve bilgileri sağlayacaktır.

#

# 6.1. OKULUMUZDA FOTOĞRAF/VİDEO ÇEKİMİ VE YAYINLANMASI

1. Okul kayıt döneminde bu metni imzalayan öğrenci velileri, fotoğraf ve video çekimi ve yayımlanması ile ilgili politikamızı da kabul etmiş sayılır. Bu metinle öğrenci fotoğraflarının okul resmî web sitesi, okul dergisi, gazete, eTwinning portalı vb. okul tanıtımlarında veli, çocuğunun sınıf resimlerinin paylaşılmasına (e-güvenliğin sağlanması koşuluyla) [Okullarda Sosyal Medya Kullanımı Genelgesi](http://alitekinsoy.meb.k12.tr/meb_iys_dosyalar/46/05/732189/dosyalar/2021_01/13042402_201712.pdf?CHK=be3af31a48bb3993ed8672653ddf2267) çerçevesinde izin verir.
2. 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. Bu yasak, bir öğrencinin diğer bir öğrencinin fotoğraf ve videosunu çekmek istemesi durumunda da geçerlidir.
3. Okul idaresi tarafından görevlendirilen kişilerin çektiği fotoğraf ve videolar ancak okulun resmî web adresinde ve sanal ortamlarında, ilgili öğrenci velisinin talep ve yazılı onayı ile yayınlanabilir. Öğrencisi için onay vermeyen velinin öğrencisi ile ilgili fotoğraf ve videolar yayınlanmaz.
4. Velisi tarafından fotoğraf ve video görüntülerinin çekilip yayınlanmasına onay verilmeyen öğrencilerin, çekim esnasında psikolojik baskı yaşamaması için tedbirler alınır.
5. Okul görevlileri tarafından yayınlanan resim ve videolarda öğrencilerin kişisel bilgilerine kesinlikle yer verilmez.

#  6.1.OKUL WEB SİTESİ VE PROJE SİTELERİNİN YÖNETİLMESİ:

1. Web sitemizde okulumuzun adres, telefon, fax ve e posta adres bilgileri bulunmaktadır.
2. Web sitesi, erişilebilirlik fikri mülkiyet haklarına saygı, gizlilik politikaları ve telif hakkı da dahil olmak üzere [Okul İnternet Siteleri Yönergesi](http://mevzuat.meb.gov.tr/dosyalar/1958.pdf) çerçevesinde yönetilecektir.
3. eTwinning projeleri kapsamında sunulan siteler sorumlu öğretmenler tarafından yine söz konusu yönergenin kapsamında idare edilecektir.
4. Öğrenci çalışmaları, velilerinin izinleriyle yayımlanacaktır.
5. Blogda; öğrenciler tarafından hazırlanacak olan bir video henüz hazırlanmadan önce, bununla ilgili görev alan öğrenciler, öğretmenlerinden izin almalıdır.
6. Paylaşılan tüm öğrenci bazlı etkinliklerde, etkinlik öncesinde velilerin izinleri alınmalıdır.
7. Canlı dersler ve çevrimiçi toplantılar, resmi veya onaylanmış uygulamalar aracılığıyla yapılacaktır.
8. Kullanıcılar, şahsi sosyal medya hesaplarında, okul öğrencileri ve çalışanlarının yer aldığı görselleri, okul yetkili mercileri tarafından onaylanmadan paylaşamazlar.
9. Çevrimiçi toplantı yapılırken, tüm kullanıcıların katılabileceği siteler üzerinden yapılacaktır.
10. Okul öğrenci ve çalışanlarını ilgilendiren/içinde bulunduran tüm içerik, ancak kontrol ve onay süreçlerinden geçtikten sonra, paylaşıma açık hale gelecektir.
11. Paylaşılan videolar liste dışı olarak paylaşılmalıdır.
12. Öğrencilerimizin okul ağını kullanarak internete erişmeleri mümkün değildir. Akıllı tahtalarımızda internet öğretmen denetiminde eğitsel amaçla kullanılmaktadır. Millî Eğitim Bakanlığı tarafından filtreleme yapılmaktadır.
13. Okul topluluğumuzun üyeleri, okul bilgisayarlarından, okulumuzun sağladığı kablosuz internet ağı haricinde bir ağa bağlanamaz.

# 7.1. İNTERNETİN/CİHAZLARIN UYGUN VE GÜVENLİ KULLANIMI:

1. 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.
2. Öğrencilerimizin okul ağını kullanarak internete erişmeleri mümkün değildir.
3. Akıllı tahtalarımızda internet öğretmen denetiminde eğitsel amaçla kullanılmaktadır. Millî Eğitim Bakanlığı tarafından filtreleme yapılmaktadır.
4. Okul topluluğumuzun üyeleri, okul bilgisayarlarından, okulumuzun sağladığı kablosuz internet ağı haricinde bir ağa bağlanamaz.
5. Öğrenciler güvenli ve doğru internet kullanımı konusunda eğitilecektir.
6. Okul, personeli ve öğrencilerin internetten materyal kullanımında telif hakkı yasalarına uygun davranabilmeleri için eğitilmeleri sağlanacaktır.
7. Öğrencilere, okudukları veya gösterilen bilgilerin doğruluğunu kabul etmeden önce eleştirel düşünmeleri öğretilecektir.
8. Çevrimiçi materyallerin değerlendirilmesi, her konuda öğretme ve öğrenmenin bir parçasıdır ve müfredatta bir bütün olarak görülür.
9. Okula ait hiçbir bilgisayar sistemi sorumsuz bir şekilde veya başkalarının işlerine engel olacak şekilde kullanılamaz.
10. Güvenilir olmayan kaynaklardan bilgisayar ve akıllı tahta sistemlerine yazılım/veri indirilemez ve yüklenemez.
11. Kurulu antivirüs programları devre dışı bırakılamaz.

# 8.1.CANLI DERS İLE İLGİLİ HUSUSLAR:

1. Harici canlı derslerde öğretmenlerimizin;
* Her ders için yeni ID ve şifre belirleyerek EBA'ya bu bilgileri girmeleri,
* Ders oluştururken "Bekleme Odası (Waiting Room)" özelliğini aktive etmeleri,
* Derse başlarken öğrencilerin isimlerini değiştirebilme seçeneklerini kapatmaları gibi basit kontrollerle benzer siber saldırılar engellenebilecektir.
1. Öğretmenlerimizin her ders için farklı ID ve şifre kullanmaları, daha önce çeşitli iletişim kanallarından paylaşılmış olan canlı ders bilgilerini geçersiz kılacaktır.
2. Öğretmenlerimiz, dersleri oluştururken "bekleme odasını" aktive ederek derse katılan öğrencileri kontrol edip böylece sahte kimlikle derse girmeye çalışan şahısların ders ortamına katılmalarını engelleyebileceklerdir.
3. Ayrıca öğretmenlerimizin, ders başlarken öğrencilerin isim değiştirmelerine olanak sağlayan özelliği devre dışı bırakmaları, böylelikle gerçek kimlikleriyle derse giren öğrencilerin sonradan bu bilgileri değiştirmelerine engel olacaktır.
4. Öğrencilerin canlı dersler sırasında dersin işlenmesine mâni olmayacak, arkadaşlarını rahatsız etmeyecek şekilde davranması esastır.
5. Öğretmenler dersin kayıt altına alındığını söylemek ve eğitsel amaçlarla politikamıza uygun olarak kullanmak koşuluyla dersleri kaydedebilir. Öğrencilerin ses ve video kaydı almasına izin verilmemektedir, öğrenciler tarafından sadece eğitsel amaçlarla ekran paylaşımı yapılan ders materyalinin ekran görüntüsü alınabilir.

 **9.1. PERSONELİN KATILIMI VE EĞİTİMİ:**

1. Çevrimiçi güvenlik (e-Güvenlik) politikası, tüm çalışanların katılımı için resmi olarak sağlanacaktır.
2. Personelimize, profesyonel ve kişisel olarak, güvenli ve sorumlu İnternet kullanımı konusunda eğitimler yapılacaktır.
3. Personelimizin çevrimiçi davranışlarının rol model olarak okuldaki öğrenciler üzerindeki öneminin farkına varması sağlanacaktır.

 **10.1. ŞİKAYETLERİN İNCELENMESİ:**

1. Okul, e-Güvenliği sağlamak için tüm gerekli önlemleri alacaktır. Bununla birlikte, internet içeriğinin uluslararası ölçeği ve doğası gereği, mobil teknolojilerin kullanımı ve değişim hızı nedeniyle, uygun olmayan materyallerin bir okul bilgisayarında veya mobil cihazda asla görünmeyeceğini garanti etmek mümkün değildir.
2. Filtreleme sistemlerimiz vardır ve okul içindeki ağımız şifre korumalıdır. Ne okul ne de bakanlık, erişilen materyal veya internet erişiminin herhangi bir sonucu için sorumluluk kabul edemez.
3. Personel ve öğrencilerin internet kullanımdaki ihlalleri ve olası sorunlar konusunda okul müdürlüğüne bilgi verilmelidir.  Herhangi bir e-güvenlik şikayeti için ilk etapta okul müdürlüğüne başvurulacaktır.
4. Okulun tüm üyeleri, çevrimiçi / siber zorbalık vb. dahil olmak üzere karşılaşılabilecek çevrimiçi risklerin çeşitliliğinden haberdar edilecektir. Bu, öğrencilere yönelik personel eğitimi ve eğitim yaklaşımları içerisinde vurgulanacaktır.
5. Okulun tüm üyeleri, filtreleme ve e-Güvenlik endişelerini bildirme prosedürü hakkında bilgilendirilecektir.
6. Okulun tüm üyeleri, gizliliğin öneminden ve endişeleri bildirmek için resmi okul usullerine uyma ihtiyacından haberdar olmalıdırlar. Okul, e-Güvenlik olaylarını, uygun olduğunda, okul disiplini / davranış politikasına uygun olarak yönetir.
7. Okulun tüm üyeleri, çevrimiçi ortamda güvenli ve uygun davranışlar gösterme, okul camiasının diğer bir üyesine zarar vermeden, suç oluşturan herhangi bir içerik, yorum, resim ve video paylaşımı yapmadan interneti kullanmaları gerektiği konusunda bilgilendirilecektir.

**Mevcut yaptırımlar şunlardır:**

* Öğrencilerle görüşme yapılması,
* Velilerin olumsuz davranışlar hakkında bilgilendirilmesi,
* Siber zorbalık şikayetleri, zorbalık karşıtı politikamıza uygun olarak ele alınması,
* [Millî Eğitim Bakanlığı Orta Öğretim Kurumları Yönetmeliği](https://www.mevzuat.gov.tr/mevzuat?MevzuatNo=18812&MevzuatTur=7&MevzuatTertip=5)'nin üçüncü bölümündeki (Disiplin) maddelerin uygulanması.