**ALPU** **ATATÜRK İLKOKULU E-GÜVENL**İ**K POL**İ**T**İ**KASI**

**Amaçlar ve politika kapsamı**

• Atatürk İlkokulu, çevrimiçi güvenliğin (e-Güvenlik), bilgisayarlar, tabletler, cep telefonları veya oyun konsolları gibi teknolojiyi kullanırken, dijital dünyadaki çocukların ve yetişkinlerin korunması için vazgeçilmez bir unsur olduğuna inanmaktadır.
• Atatürk İlkokulu, internetin ve bilgi iletişim teknolojilerinin günlük yaşamın önemli bir parçası olduğuna inanır. Dolayısıyla, riskleri yönetmeleri ve bunlara tepki vermek için stratejiler geliştirmenin yollarını öğrenmeleri için çocuklar desteklenmelidir.
• Atatürk İlkokulu, eğitim standartlarını yükseltmek, başarıyı teşvik etmek, personelin mesleki çalışmalarını desteklemek ve yönetim işlevlerini geliştirmek için toplumun kaliteli internet erişimi sunma yükümlülüğüne sahiptir.
• Atatürk İlkokulu, tüm çocukların ve personelin çevrimiçi olarak potansiyel zararlardan korunmasını sağlamakla sorumludur.
• Bu politika, yöneticiler, öğretmenler, destek personeli, çocuklar ve ebeveynler için hazırlanmıştır.
• Bu politika, internet erişimi ve kişisel cihazlar da dahil olmak üzere bilgi iletişim cihazlarının kullanımı için geçerlidir; çocuklar, personel ya da diğer kişilere, çalıştıkları dizüstü bilgisayarlar, tabletler veya mobil cihazlar gibi uzaktan kullanım için okul tarafından verilen cihazlar için de geçerlidir.

**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 eğitimini ilişkilendirmek.
• Okul koruma politikalarını ve prosedürlerini takip ederek endişe duyan/duyulan bireyleri belirlemek ve önlem almak.
• Olumlu öğrenme fırsatlarına vurgu yapmak.
• Bu alanda mesleki gelişim için kişisel sorumluluk almak.

**Çocukların başlıca sorumlulukları şunlardır:**

• Çevrimiçi güvenlik politikalarının geliştirilmesine katkıda bulunmak.
• Okulun Kabul Edilebilir Kullanım Politikalarını okumak ve onlara bağlı kalmak.
• 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.
• 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.

**Ebeveynlerin başlıca 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.
• 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.
• Öğrenme platformları ve diğer ağ kaynakları gibi okul sistemlerini güvenli ve uygun bir şekilde kullanmak.
• Yeni ve gelişmekte olan teknolojilerin getirdiği fırsatlar ve risklerle ilgili olarak kendi bilinci ve öğrenimlerinden sorumlu olmak.

**Okul / web sitesinin yönetilmesi:**

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

**Çevrimiçi görüntü ve videolar yayınlama**:
• Okul, çevrimiçi paylaşılan tüm resimlerin ve videoların okul resim kullanımı politikasına uygun şekilde kullanılmasını sağlayacaktır.
• Okul, resimlerin ve videoların tümünün, veri güvenliği, Kabul Edilebilir Kullanım Politikaları, Davranış Kuralları, sosyal medya, kişisel cihazların ve cep telefonlarının kullanımı gibi diğer politikalar ve prosedürlere uygun şekilde yer almasını sağlayacaktır.
• Görüntü politikasına uygun olarak, öğrencilerin resimlerinin / videolarının elektronik olarak yayınlanmasından önce her zaman velilerden remi yazılı izni alınacaktır.

**Eğitim amaçlı resmi video konferans ve web kamerası kullanımı**:
• Okul, video konferansın çok çeşitli öğrenme avantajlarıyla zorlu bir faaliyet olduğunu kabul eder. Hazırlık ve değerlendirme, tüm faaliyet için gereklidir.
• Tüm video konferans ekipmanları, kullanılmadığında ve uygun olduğunda kapatılacaktır, otomatik cevaplamaya ayarlanmayacaktır.
• Harici IP adresleri diğer sitelere sunulmayacaktır.
• Video konferans iletişim detayları kamuoyuna açık olarak paylaşılmayacaktır.
• Video konferans ekipmanları güvenli bir şekilde tutulacak ve gerekirse kullanılmadığında kilitlenecektir.
• Okul video konferans ekipmanları izinsiz olarak okul binalarından çıkarılmayacaktır.
• Personel, dış video konferans fırsatlarının ve / veya araçlarının uygun bir şekilde değerlendirildiğinden emin olacak ve olaylara erişmek için kullanılan hesapların ve sistemlerin uygun bir şekilde güvenli ve gizli olmasını sağlayacaktır.

**Kullanıcılar**
• Öğrenciler, bir video konferans araması veya mesajı hazırlamadan veya cevaplamadan önce bir öğretmenin izin isteyecektir.
• Video konferans, öğrencilerin yaşı ve yeteneği için uygun bir şekilde denetlenecek.
• Velilerin rızası, çocuklar video konferans faaliyetlerine katılmadan önce alınacaktır.
• Video konferans, sağlam bir risk değerlendirmesini takiben, resmi ve onaylanmış iletişim kanalları vasıtasıyla gerçekleşecektir
• Sadece ana yöneticilere video konferans yönetim alanlarına veya uzaktan kumanda sayfalarına erişim hakkı verilecektir.
• Eğitimsel video konferans servisleri için özel oturum açma ve şifre bilgileri yalnızca personellere verilecek ve gizli tutulacak.

**İçerik**
• Bir video konferans dersi kaydederken, tüm siteler ve katılımcılar tarafından yazılı izin alınacaktır. Konferansın başlangıcında kayıt nedeni belirtilmeli ve video konferans kaydı tüm taraflara açık olmalıdır. Kaydedilen malzemeler güvenli bir şekilde saklanacaktır.
• Üçüncü taraf materyalleri dahil edilecekse, okul üçüncü şahsın fikri mülkiyet haklarını ihlal etmekten kaçınmak için bu kaydın kabul edilebilir olup olmadığını kontrol edecektir.
• Okul, bir video konferansa katılmadan önce diğer konferans katılımcılarıyla diyalog kuracak. Okul değilse, okul sınıf için uygun olan materyali teslim aldığını kontrol edecektir.

**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 tasarlanacaktır.
• İnternet erişim seviyeleri müfredat gerekliliklerini ve öğrencilerin yaş ve yeteneklerini yansıtacak şekilde gözden geçirilecektir.
• Çalışanların tüm üyeleri, çocukları korumak için tek başına filtrelemeye güvenmeyeceklerinin farkındadır ve gözetim, sınıf yönetimi ve güvenli ve sorumlu kullanım eğitimi önemlidir.
• Öğrencilerin yaşlarına ve yeteneklerine uygun olacaktır.
• Tüm okul 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 değerlendirecektir.
• Öğrenciler, bilginin konumlanması, alınması ve değerlendirilmesi becerileri de dahil olmak üzere, internette araştırmada etkili kullanımı konusunda eğitilecektir.
• Okul, personelin ve öğrencilerin İnternet´ten türetilen materyallerin telif hakkı yasalarına uygun olmasını ve bilgi kaynaklarını kabul etmesini sağlayacaktır.
• Öğrencilere, okudukları veya gösterilen bilgilerin doğruluğunu kabul etmeden önce eleştirel düşünmeleri öğretilecektir.
• Çevrimiçi materyallerin değerlendirilmesi, her konuda öğretme ve öğrenmenin bir parçasıdır ve müfredatta bir bütün olarak görülür.
• Okul, öğrencileri ve çalışanlarımızın güvenli ve gizli bir ortamda iletişim kurmalarını ve işbirliği yapmalarını sağlamak için interneti kullanacaklardır.

**Kişisel Cihazların ve Cep Telefonlarının Kullanımı:**

• Cep telefonlarının ve çocukların, gençlerin ve yetişkinler arasındaki diğer kişisel cihazların yaygın bir şekilde sahiplenilmesi, tüm üyelerin Atatürk İlkokulu topluluğunun cep telefonlarının ve kişisel cihazların sorumlu bir şekilde kullanılmasını sağlamak için gerekli adımları atmalarını gerektirir.
• 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.
• Atatürk İlkokulu, 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.

**Kişisel cihazların ve cep telefonlarının güvenli bir şekilde kullanılması için beklentiler**

• Kişisel cihazların ve cep telefonlarının kullanımı yasaya ve diğer uygun okul politikalarına uygun olarak yerine getirilecektir.
• Sahaya getirilen her türlü elektronik cihazın sorumluluğu kullanıcıya aittir. Okul, bu tür öğelerin kaybı, çalınması veya zarar görmesi konusunda sorumluluk kabul etmez. Okul, bu tür cihazların potansiyel veya fiili neden olduğu olumsuz sağlık etkileri için sorumluluk kabul etmez.
• Kötüye kullanım veya uygun olmayan mesajların veya içeriğin cep telefonları veya kişisel cihazlarla gönderilmesi, topluluğun herhangi bir üyesi tarafından yasaklanır ve herhangi bir ihlal, disiplin / davranış politikasının bir parçası olarak ele alınacaktır.
• Atatürk İlkokulu topluluğunun tüm üyelerine cep telefonlarını veya cihazlarını kayıp, hırsızlık veya hasardan korumak için adım atmaları önerilir.
• Atatürk İlkokulu topluluğunun tüm üyelerinden, kayboldukları veya çalındığı takdirde yetkisiz aramaların veya hareketlerin telefonlarında veya cihazlarında yapılamayacağından emin olmak için şifreler / pin numaraları kullanmaları önerilir. Parolalar ve pin numaraları gizli tutulmalıdır. Cep telefonları ve kişisel cihazlar paylaşılmamalıdır.
• Atatürk İlkokulu topluluğunun tüm üyelerine, cep telefonlarının ve kişisel cihazlarının saldırgan, küçümseyen veya başka şekilde okul / ayar politikalarına aykırı düşen herhangi bir içerik içermediğinden emin olmaları önerilir.

**Öğrencilerin kişisel cihazlar ve cep telefonları kullanımı**
• Öğrenciler, kişisel cihazların ve cep telefonlarının güvenli ve uygun kullanımı konusunda eğitim alacaklardır.
• Çocukların cep telefonlarının ve kişisel cihazların tüm kullanımları, kabul edilebilir kullanım politikasına uygun olarak gerçekleşecektir.
• Cep telefonları veya kişisel cihazlar, öğrencilerin bir öğretim üyesinin onayını alarak onaylanmış ve yönlendirilmiş müfredat tabanlı etkinlik kapsamında olmadıkları sürece dersler veya resmi okul saatlerinde öğrenciler tarafından kullanılamaz.
• Çocukların cep telefonlarını veya kişisel cihazlarını eğitim etkinliğinde kullanımı, okul idaresi tarafından onaylandığında gerçekleşecektir.
• Bir öğrenci ebeveynlerini arama gereği duyduğunda, okul telefonunu kullanmasına izin verilecektir.
• Ebeveynlerin okul saatlerinde cep telefonuyla çocuklarıyla iletişim kurmamaları, okul idaresine başvurmaları önerilir. İstisnai durumlarda öğretmenin onayladığı şekilde istisnalara izin verilebilir.
• Öğrenciler, telefon numaralarını yalnızca güvenilir arkadaşlarına ve aile üyelerine vermelidirler.
• Öğrencilere, cep telefonlarının ve kişisel cihazların güvenli ve uygun bir şekilde kullanımı öğretilecek ve sınırların ve sonuçların farkına varılacaktır.
• 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.

**Personelin kişisel cihazlar ve cep telefonları kullanımı**
• Personelin, kendi kişisel telefonlarını veya cihazlarını, çocukların, gençlerin ve ailelerinin, mesleki bir kapasitede, ortamın içinde veya dışındaki bölgeleriyle bağlantı kurmalarına izin verilmez. Bu konuyu tehlikeye atacak önceden var olan ilişkiler yöneticilerle görüşülecektir.
• Personel, çocukların fotoğraflarını veya videolarını çekmek için cep telefonları, tabletler veya kameralar gibi kişisel cihazları kullanmaz ve yalnızca bu amaçla izin verilen ekipmanı kullanır.
• Personel herhangi bir kişisel cihazı doğrudan çocuklarla kullanmaz ve ders / eğitim etkinlikleri sırasında yalnızca okul tarafından sağlanan ekipmanı kullanır.
• Personel, kişisel telefonların ve cihazların herhangi bir şekilde kullanımının daima veri koruma ve ilgili okul politikası ve prosedürleri uyarınca yerine getirilmesini sağlayacaktır.
• Personel kişisel cep telefonları ve cihazları ders saatlerinde kapatılıp / sessiz moda geçirilir.
• Bluetooth veya diğer iletişim biçimleri ders saatlerinde kapalı olmalıdır.
• Acil durumlarda okul idaresi tarafından izin verilmemişse, kişisel cep telefonları veya cihazları öğretim dönemleri boyunca kullanılamaz.
• Personel, cep telefonları ve kişisel cihazlar üzerinden sitede satın alınan içeriğin profesyonel rolü ve beklentileri ile uyumlu olmasını sağlayacaktır.
• Bir personel okul politikasını ihlal ettiği durumlarda disiplin işlemi yapılır.
• Bir personelin, bir cep telefonuna veya kişisel bir cihaza kaydedilen veya saklanan yasadışı içeriğe sahip olduğu veya ceza gerektiren bir suç işlemiş olması durumunda, polise ulaşılacaktır. • Personelin cep telefonunu veya cihazlarını kişisel olarak kullanmalarını içeren herhangi bir iddiaya okul yönetim politikasını izleyerek yanıt verilecektir.

**Ziyaretçi kişisel cihazların ve cep telefonlarının kullanımı**•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.•Personelin uygun ve güvenli olduğunda sorunlara karşı çıkması ve her zaman ziyaretçilerin herhangi bir ihlalini idareye bildirmeleri beklenmektedir.

**Çocukların 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.
• Güvenli ve sorumlu kullanım ile ilgili eğitim internet erişiminden önce yapılacaktır.
• 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.
• Çevrimiçi güvenlik (e-Güvenlik) PSHE, SRE, Citizenshipand Computing / BİT programlarına dahil edilecek ve hem güvenli okul hem de evde kullanımını kapsayacaktır.
• Kabul Edilebilir Kullanım beklentileri ve posterler, okul binasında uygun görülen her yerde yayınlanacaktır.
• İnternetin ve teknolojinin güvenli ve sorumlu kullanımı, müfredatta ve tüm konularda güçlenecektir.
• Dışarıdan destek, okulların dahili çevrimiçi güvenlik (e-Güvenlik) eğitim yaklaşımlarını tamamlamak ve desteklemek için kullanılacaktır.
• Okul, öğrencilerin teknolojiyi olumlu şekilde kullandıklarını ödüllendirecektir.
• Okul, öğrencilerin ihtiyaçlarına uygun olarak çevrimiçi güvenliği geliştirmek için akran eğitimini uygulayacaktır.
• Okulda Güvenli İnternet Günü (SID) kutlanacak ve yapılacak etkinliklerle güvenli internet hakkında bilgi verilecektir.

**Personelin eğitimi**

• 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 tek bir kullanıcıya kadar izlenebileceğinin farkında olarak okul sistemlerini ve cihazlarını kullanırken takdir yetkisi ve profesyonel davranış gösterecektir.
• Personelin tüm üyelerine, profesyonel ve kişisel olarak, güvenli ve sorumlu internet kullanımı konusunda güncel ve uygun personel eğitimi, düzenli temelde çeşitli şekillerde sağlanacaktır.
• Çalışanların tüm üyeleri, çevrimiçi davranışlarının okuldaki rolü ve itibarını etkileyebileceğinin farkına varacaktır. Mesleki veya kurum itibarını düşürmeye yönelik veya profesyonel yeteneklerine güvenin kaybedilmesini gerektiren bir şeyin bulunduğu düşünülürse, kamusal, disiplin veya hukuki önlemler alınabilir.
• Filtreleme sistemlerini yönetme veya BİT kullanımını izleme sorumluluğu taşıyan personelin üyeleri, idare tarafından denetlenecek ve sorunları veya endişeleri bildirmek için açık prosedürlere sahip olacaklardır.
• Okul, çalışanların, öğrencilerin yaşlarına ve yeteneklerine göre kullanması gereken yararlı çevrimiçi araçları vurgulamaktadır.

**Ebeveynlerin eğitimi**

• Atatürk İlkokulu, çocukların internetin ve dijital teknolojinin güvenilir ve sorumlu kullanıcıları olabilmesi için ana-babaların oynayacakları önemli bir role sahip olduklarını kabul eder.
• Ebeveynlerin dikkatleri, okul açıklamaları ve okul web sitesinde okul çevrimiçi güvenlik (e-Güvenlik) politikasına ve beklentilerine yöneltilecektir.
• Ebeveynlerin çevrimiçi güvenlik bilgilerini okumaları istenecektir.
• Ebeveynler, Okul Kabul Edilebilir Kullanım Politikasını okumaya ve çocuklarıyla etkilerini tartışmaya teşvik edilecektir.
• Çevrimiçi güvenlik konusundaki bilgi ve rehberlik, ebeveynlere çeşitli biçimlerde sunulacaktır.
• Ebeveynlerin, çevrimiçi olarak çocukları için olumlu davranışları rol modellemeleri teşvik edilecektir.

**Çevrimiçi Olaylara ve Koruma sorunlarına yanıt verme**
• Okulun tüm üyeleri, cinsel içerikli mesajlaşma, çevrimiçi / siber zorbalık vb. dahil olmak üzere karşılaşılabilecek çevrimiçi risklerin çeşitliliğinden haberdar edilecektir. Bu, öğrencilere yönelik personel eğitimi ve eğitim yaklaşımları içerisinde vurgulanacaktır.
• Okulun tüm üyeleri, filtreleme, cinsel içerikli mesajlaşma, siber zorbalık, yasadışı içerik ihlali vb. gibi çevrimiçi güvenlik (e-Güvenlik) endişelerini bildirme prosedürü hakkında bilgilendirilecektir.
• Dijital Abone Hattı (DSL), daha sonra kaydedilecek olan çocuk koruma endişelerini içeren herhangi bir çevrimiçi güvenlik (e-Güvenlik) olayı hakkında bilgilendirilecektir.
• İnternetin yanlış kullanımı ile ilgili şikâyetler, okulun şikâyet prosedürleri kapsamında ele alınacaktır.
• Çevrimiçi / siber zorbalık ile ilgili şikayetler, okulun zorbalık karşıtı politikası ve prosedürü kapsamında ele alınacaktır.
• Personelin interneti yanlış kullanımı ile ilgili herhangi bir şikayet okul müdürüne yönlendirilecektir.
• Okul şikayet prosedürü öğrencilere, velilere ve personele bildirilecektir.
• Şikayet ve ihbar prosedürü personele bildirilecektir.
• Okulun tüm üyeleri, gizliliğin öneminden ve endişeleri bildirmek için resmi okul usullerine uyma ihtiyacından haberdar olmalıdırlar.
• Okulun tüm üyelerine; çevrimiçi ortamda güvenli ve uygun davranış hakkında hatırlatma yapılacak ve okul camiasının herhangi bir diğer üyesine zarar vermek, sıkıntı yaşatmak veya suç oluşturan herhangi bir içerik, yorum, resim veya video yayımlamamanın önemi hatırlatılacaktır.
• Okul, çevrimiçi güvenlik (e-Güvenlik) olaylarını, uygun olduğunda, okul disiplin/davranış politikasına uygun olarak yönetir.
• Okul, ebeveynlere, ihtiyaç duyulduğunda bunlarla ilgili endişeleri bildirir.
• Herhangi bir soruşturma tamamlandıktan sonra okul bilgi alacak, öğrenilen dersleri belirleyecek ve değişiklikleri gerektiği gibi uygulayacaktır.
• Sorunları çözmek için ebeveynlerin ve çocukların okulla ortak çalışması gerekmektedir.

**Kabul Edilebilir Kullanım Politikası**

Alpu Atatürk İlkokulu bilgisayar sistemlerini onlarca kullanıcı paylaşmaktadır. Bu sistemler dikkatli bir şekilde kullanılmadığı takdirde okulun ve diğer kişilerin çalışmalarını sekteye uğratma potansiyeline sahiptir. Bu sebeple kullanıcılar okulun bilgisayar sistemlerini kullanırken dikkatli olmalı ve etik davranış sergilemelidir. Bu yükümlülük, aşağıdakilerle sınırlı olmamakla birlikte şunları kapsamaktadır:

* Okul, okula ait bilgisayar sistemleri üzerindeki tüm hak, mülkiyet ve çıkarlara sahiptir. Atatürk İlkokulu  Kabul Edilebilir Kullanım Politikası veya bilgisayar sistemlerinin kullanımına ilişkin olarak okul tarafından herhangi bir mecrada yayımlanan hüküm ve koşullar altındaki hiçbir hüküm hiçbir şekilde söz konusu hak, mülkiyet ve çıkarların kullanıcılara devredildiği anlamına gelmemektedir.
* Okul kullanıcılara sadece bilgisayar sistemlerinin kullanımına ilişkin şahsi, dünya genelinde, bedelsiz, devredilemeyen ve münhasır olmayan bir lisans tanımaktadır. Kullanıcılar bilgisayar sistemlerinin hiçbir yazılım veya diğer bir parçasını kopyalayamaz, değiştiremez, yeniden üretemez, bunlardan türemiş çalışma yaratamaz, tersine mühendislik yapamaz, parçalara ayıramaz veya diğer bir şekilde kaynak koduna dönüştüremez.
* Kullanıcılar, okulun izin vermediği bilgisayar sistemlerini kullanamazlar. Bilgisayar sistemlerine erişebilmek için hatalı veya aldatıcı bilgilerin temin edilmesi suretiyle veya sair şekillerde bilgisayar sistemlerinin yetkisiz kullanımı yasaktır. Kullanıcılar diğer kurum, kuruluş veya kişilerin bilgisayar sistemlerine yetkisiz erişim sağlamak için okulun bilgisayar sistemlerini kullanamaz.
* Kullanıcılar, okul hesaplarını kullanması için hiç kimseyi hiçbir sebeple yetkilendiremez. Okul hesabının her türlü kullanımından hesap sahibi sorumludur. Kullanıcılar hesaplarının yetkisiz kişilerce kullanılmasının önüne geçilmesi için şifre koruma ve belge koruma dâhil tüm makul önlemleri almalıdır. Şifrelerini başka bir kişiyle paylaşmamalı ve şifrelerini düzenli olarak değiştirmelidir. Bir kullanıcı hesabına ait şifre kullanılarak gerçekleştirilen her türlü işlemden, söz konusu işlemi gerçekleştiren taraf hesap sahibinin kendisi olmasa dahi sorumlu hesap sahibidir.
* Okulun bilgisayar sistemleri yalnızca izin verildiği şekilde, okul ile ilişkili hususlarda kullanılmalıdır. Tüm okul donanımı için söz konusu olduğu üzere, okul ağı dâhil bilgisayar sistemlerinin şahsi veya ticari amaçlar doğrultusunda kullanılması, açıkça izin verilmeyen haller dışında yasaktır. Okulun bilgisayar sistemleri, hileli ya da hukuka aykırı bir şekilde elde edilmiş medya belgeleri ile yazılımların toplanması, yüklenmesi, dağıtılması dâhil ve bunlarla sınırlı olmamak üzere hiçbir hukuka aykırı amaç için kullanılamaz. Dış ağ veya hizmetlerin – bulut hizmetleri dâhil – kullanımı hem okul hem de söz konusu ağ ve hizmetleri sunan kuruluşlar tarafından yayımlanan kabul edilebilir kullanım politikalarına uygun olmalıdır.
* Kullanıcılar okulun ilgili personeli, bilgi güvenliği sorumlusu veya ilgili taraftan önceden izin almadıkça, herhangi bir bilgiye, okula ait yazılıma veya diğer belgelere (programlar, altyordam kitaplığı üyeleri, veri ve elektronik posta dâhil) erişemez; söz konusu bilgi, yazılım ve belgeleri değiştiremez, kopyalayamaz, taşıyamaz veya kaldıramaz. Kullanıcılar lisans verenden önceden izin almadıkça, üçüncü kişilere ait yazılımları kopyalayamaz, dağıtamaz, görüntüleyemez veya açıklayamaz. Kullanıcılar kullanımı için uygun bir şekilde lisanslanmamış olan yazılımları sistemlere yükleyemez.
* Okula ait hiçbir bilgisayar sistemi sorumsuz bir şekilde veya başkalarının işlerine engel olacak şekilde kullanılamaz. Buna; hakaret içerikli, rahatsız edici veya taciz edici içerikler ile zincirleme mektup, yetkisiz toplu mail veya istenmeyen reklamların iletilmesi veya ulaşılabilir kılınması; kullanıcıya ait olmayan bir sistem, materyal veya bilgiye kasıtlı, dikkatsizce veya ihmalkâr bir biçimde zarar verilmesi; kasıtlı olarak elektronik iletişimin kesintiye uğratılması veya diğer bir şekilde başkalarının mahremiyetinin ihlal edilmesi veya kullanıcıya ait olmayan veya kullanıcı için olmayan bilgiye erişilmesi; sistem kaynaklarının kasıtlı olarak hatalı kullanılması veya başkalarının hatalı kullanmasının sağlanması veya ücretsiz yazılım gibi güvenilir olmayan kaynaklardan idari sistemlere yazılım veya veri indirilmesi dâhildir.
* Okul, bilgisayar sistemlerine bizzat sağlamadığı içeriklerden hiçbir şekilde sorumlu değildir. Kullanıcılar başkaları tarafından verilen içeriklere, bunların hakaret içerici, uygunsuz veya sakıncalı olduğunu düşünebileceğini kabul ederek ve risk kullanıcının kendisine ait olmak üzere erişir. Bilgisayar sistemleri "OLDUĞU GİBİ" ve "MEVCUT HALİYLE" sunulmaktadır. Okul, üçüncü taraf içeriklerinin doğru, tam ve güvenilir olduğuna ilişkin her türlü yükümlülükten kendini muaf tutmaktadır. Kullanıcı bilgisayar sistemlerinde bulundurduğu veya sakladığı bilgilerden kendisi sorumludur.
* Kullanıcı (i) bilgisayar sistemlerinin işleyişini veya söz konusu bilgisayar sistemlerinin başkaları tarafından kullanımını engelleyici her türlü harekete teşebbüsün; (ii) bilgisayar sistemlerine fazla yükleme yapacak içeriklerin yüklenmesinin; (iii) bilgisayar sistemlerinin genel güvenliğine tehlike arz edecek ve/veya diğer kullanıcıları zarara uğratacak hareketlerin; (iv) bilgisayar sistemlerinin işleyişini engelleyici veya müdahale edici yazılımların kullanılmasının veya kullanılmaya çalışılmasının mutlak bir biçimde yasak olduğunu kabul eder.
* İşbu politikanın başka bir kişi tarafından ihlaline veya bilgisayar sistemlerinin güvenliği ile ilgili bir hata ya da güvenliğin ihlal edilmesine ilişkin her türlü bilginin tespiti durumunda, vakanın E-Güvenlik Koordinatörlüğü'ne bildirilmesi zorunludur.
* Okul bilgisayar sistemlerinin yetkisiz veya uygunsuz bir şekilde kullanımı, işbu politikaya uyulmaması dâhil, Okul politikasının ihlalini teşkil etmektedir ve idare onayıyla Disiplin Kurulu takibini gerektirir. İşbu politikaya veya politikanın belli bir duruma uygulanmasına ilişkin her türlü soru E-Güvenlik Koordinatörlüğü'ne iletilir.