



# BAĞLİCA ANADOLU LİSESİ

## E-SAFETY POLİTİKASI

### İLETİŞİM

03125036064

baglicaanadolu@gmail.com

<https://baglicaanadolulisesi.meb.k12.tr>

Bağlıca Mahallesi Kuzupınarı Caddesi No 1/A

Etimesgut / Ankara

Durmuş KANIŞ

Okul Müdürü

Günümüzde internet kullanımı yaşamın ayrılmaz bir parçasıdır. İnternetin doğru, verimli ve güvenli kullanılabilmesi amacıyla Bağlıca Anadolu Lisesi “Okul Güvenlik Politikası” oluşturuldu.

Okulumuzda öğretim süreçlerinin gerçekleştirilmesinde internetten yararlanılmaktadır. Eğitim öğretim süreçlerinde öğrenci, öğretmen, veli ve personelimiz gibi paydaşlarımız okulumuzda internete erişebilirler. Paydaşlarımızın sürekli gelişim hâlinde olan dijital teknolojiler aracılığıyla üretilen programların verimli ve güvenli kullanmalarını sağlamak amacıyla e güvenlik okul politikası oluşturuldu.

Okulumuz e güvenlik politikasının amaçlarını paydaşlarımıza benimsetmek için bulunabilecekleri her ortamda farkındalığını kavrayabilecekleri Güvenli İnternet Okul Politikasına sahiptir.

## **E-GÜVENLİK (E-SAFETY) POLİTİKAMIZ**

Okulumuzda dersler etkileşimli tahta ve MEB interneti kullanılarak yapılır. Ders anlatımlarında EBA portalından yararlanır. MEB internet erişiminin güvenliği güvenlik filtresiyle sağlanır.

Okulumuzun web sitesi, Instagram ve Youtube hesapları bulunmaktadır. Bu hesaplar üzerinden yayınlanan veriler okul web komisyonu tarafından kontrolü yapılarak paylaşılır.

Etkileşimli tahtalar e-kilit güvenlik programları ile Bilişim Teknolojileri Rehber öğretmenin periyodik kontrolünde kullanılır.

Okulumuzda öğrencilerin cep telefonları ilk ders saatinde toplanarak son ders saati sonuna kadar kapalı konumda tutulur.

Okulumuzda "Daha Güvenli İnternet Günü" kutlanır.

Okulumuzda Bilgi İletişim Teknolojileri (BİT) araçlarının doğru ve güvenli kullanımı ile ilgili sabit panolarda bilgilendirme yapılır.

Okulumuzda Rehberlik servisinin tüm sınıflar düzeyinde düzenli olarak organize ettiği BİT bağımlılığı, BİT'nin doğru ve güvenli kullanımı, Siber Zorbalık, internet güvenliği vb. konularda seminerler düzenlenir. Bu seminerler BİT uzmanları veya emniyet görevlileri tarafından verilir.

Rehberlik servisi tarafından öğrencilerimize, <https://tbm.org.tr> internet adresinde yer alan "Teknoloji Bağımlılığı" içerikleri düzenli olarak uygulanır.

Okulumuzun öğretmenleri, Milli Eğitim Bakanlığı (MEB) tarafından verilen Siber Zorbalık, BİT'in doğru ve güvenli kullanımı konularında uzaktan ve yüz yüze eğitimler alarak konuyla ilgili farkındalıkları artırılır.

Velilerimize internetin doğru ve güvenli kullanımı ile ilgili uzaktan seminerler verilir.

Okulumuz web sitesinde öğretmen ve öğrencilerimizin kişisel bilgileri e-güvenik içeriğine uygun olarak paylaşılır.

Okulumuza yeni kayıt hakkı kazanan öğrencilerimize 6698 sayılı "Kişisel Verilerin Korunması" kanunu kapsamında bilgilendirme yapılır.

## **E-GÜVENLİK (E-SAFETY) POLİTİKAMIZIN AMACI**

Okulumuzun tüm paydaşlarını çevrimiçi olarak korumak ve güvenliğini sağlamak,

Teknolojinin potansiyel riskleri ve yararları konusunda Bağlıca Anadolu Lisesi idareci, öğretmen, öğrenci ve çalışanları için farkındalık oluşturmak,

Tüm personelin güvenli ve sorumlu bir şekilde çalışmasını sağlamak, olumlu davranışları çevrimiçi olarak modellemek ve teknolojiyi kullanırken kendi standartlarını ve uygulamalarını yönetme gereksiniminin farkında olmak.

Okuldaki tüm üyeler tarafından bilinen çevrimiçi güvenlik endişelerine yanıt verirken açıkça kullanılacak prosedürleri tanımlamak.

e-güvenlik politikasının tüm paydaşları (yönetim organı, öğretmenler, destek personeli, harici yükleniciler, ziyaretçiler, gönüllüler, okul adına hizmet veren veya bunları yerine getiren diğer kişiler, öğrenciler ve ebeveynleri) kapsamını sağlamak.

e-güvenlik politikası, internet erişimi ve kişisel cihazlar da dâhil olmak üzere tüm bilgi iletişim cihazlarının kullanımı için geçerlidir.

## **SORUMLULUKLARIMIZ**

- ❖ Çevrimiçi güvenlik politikalarının geliştirilmesine katkıda bulunmak.
- ❖ Kabul Edilebilir Kullanım Politikalarını (AUP) okumak ve onlara bağlı kalmak.
- ❖ Okul sistemlerinin ve verilerin güvenliğinden sorumlu olmak.
- ❖ Çevrimiçi güvenlik konusundaki farkındalığa sahip olmak.
- ❖ 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 bireyleri belirlemek ve uygun önlemleri almak.
- ❖ Olumlu öğrenme fırsatlarına vurgu yapmak.
- ❖ Bu alanda mesleki gelişim için kişisel sorumluluk almak

## ÖĞRENCİLERİMİZİN SORUMLULUKLARI

- ❖ Çevrimiçi güvenlik politikalarının geliştirilmesine katkıda bulunmak.
- ❖ Okulun Kabul Edilebilir Kullanım Politikalarını okumak ve onlara bağlı kalmak.
- ❖ Çevrimiçi ve çevrimdışı başkalarının hislerine ve haklarına saygı duymak.
- ❖ İşler ters giderse, güvenilir bir yetışkenden yardım istemek ve çevrimiçi güvenlik sorunlarıyla karşılaşan diđer kişileri desteklemek.
- ❖ Kendilerini ve başkalarını çevrimiçi olarak korumak için sorumluluk almak.
- ❖ Yeni ve gelişmekte olan teknolojilerin getirdiđi 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.
- ❖ Bireysel yaşlarına, yeteneklerine ve zayıf yönlerine uygun bir seviyede davranmak.

## EBEVEYNLERİN SORUMLULUKLARI

- ❖ 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, çocuđun çevrimiçi olarak zarar görme tehlikesi altında olduğunu gösteren deđişiklikleri belirlemek.
- ❖ Kendileri veya çocukları çevrimiçi problem veya sorunlarla karşılaşırsa okul veya diđer uygun kurumlardan yardım veya destek istemek.
- ❖ Okulun çevrimiçi güvenlik politikalarının oluşturulmasına katkıda bulunmak.
- ❖ Öğrenme platformları ve diđer ağ kaynakları gibi okul sistemlerini güvenli ve uygun bir şekilde kullanmak.
- ❖ Yeni ve gelişmekte olan teknolojilerin getirdiđi fırsatlar ve risklerle ilgili olarak kendi bilinci ve öğrenimlerinden sorumlu olmak.

## **ÇEVİRİMİÇİ İLETİŞİM VE TEKNOLOJİNİN DAHA GÜVENLİ KULLANIMI**

### **OKUL WEB SİTESİNİN YÖNETİLMESİ**

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 dâhil 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 dâhil olmak üzere, toplumun üyeleri için okul web sitesinde korunma hakkında bilgi gönderecektir.

### **ÇEVİRİMİÇİ GÖRÜNTÜ VE VİDEO YAYINLAMAK**

Okul, çevrimiçi paylaşılan tüm fotoğrafların ve videoların okul veri güvenliği politikasına uygun şekilde kullanılmasını sağlayacaktır.

Okul, fotoğrafların 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 fotoğraflarının ve videolarının dijital ortamda yayınlanabilmesi için ebeveynlerin yazılı izni alınacaktır.

### **VİDEO KONFERANS KURALLARI**

Öğrenciler, bir video konferans araması/mesajı hazırlamadan veya cevaplamadan önce görevli öğretmenden izin isteyecektir.

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

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 ilgililere verilecek ve gizli tutulacak.

Öğrencilerin video konferans faaliyetleri için ebeveyn izinleri alınacaktır.

## **KİŞİSEL CİHAZLARIN VE CEP TELEFONLARININ KULLANIMI**

Cep telefonlarının ve kişisel cihazların sorumlu bir şekilde kullanılmasını sağlamak için gerekli adımları atmak.

Gençlerin ve yetişkinlerin cep telefonlarının ve diğer kişisel cihazların kullanımı, okul tarafından kararlaştırılacak ve okul Kabul Edilebilir Kullanım veya Cep Telefonu Politikası dâhil olmak üzere uygun politikalarda yer alacaktır.

Bağlıca Anadolu Lisesi, mobil teknolojilerle yapılan kişisel iletişimin, paydaşlar için gündelik yaşamın kabul edilen bir parçası olduğunun farkındadır; ancak, bu tür teknolojilerin okulda güvenli ve uygun bir şekilde kullanılmasını sağlar.

## **ÖĞRENCİLERİN KİŞİSEL CİHAZLARI VE CEP TELEFONLARINI KULLANIMI**

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

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.

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

Öğrenciler ders başlamadan önce telefonlarını okul yönetimi tarafından yaptırılan telefon dolaplarına koymakla yükümlüdür. Cep telefonunun amacı dışında kullanımı ihlâli 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. Velisi dışında telefon kimseye teslim edilmez.

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.

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 varmaları sağlanacaktır.

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.

## **PERSONELİN KİŞİSEL CİHAZLARI VE CEP TELEFONLARINI KULLANIMI**

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 kapatılır/sessiz moda geçirilir.

Bir personel okul politikasını ihlâl ettiği durumlarda soruşturma işlemi yapılır.

Bir personelin, bir cep telefonuna veya kişisel bir cihaza kaydedilen veya saklanan yasa dışı içeriğe sahip olduğu veya ceza gerektiren bir suç işlemiş olması durumunda, polise ulaşılabacaktır.

Personelin cep telefonunu veya cihazlarını kişisel olarak kullanmalarını içeren herhangi bir iddiaya okul yönetim politikasını izleyerek yanıt verilecektir.

## **ZİYARETÇİLERİN KİŞİSEL CİHAZLARI VE CEP TELEFONLARINI KULLANIMI**

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.

3. kişilerin okul binası içinde fotoğraf, video çekimi yapması yasaktır

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

Personel, ziyaretçilerin her hangi bir ihlâli ile karşılaştığında sorunu idareye bildirecektir.

## **ÇOCUKLARIN VE GENÇLERİN KATILIMI VE EĞİTİMİ**

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 dâhil 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.

Kabul Edilebilir Kullanım Politikaları beklentileri ve posterler, internet erişimi olan tüm odalarda yayınlanacaktır.

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

Okulun dâhili çevrimiçi güvenlik (e-Güvenlik) eğitim yaklaşımlarını tamamlamak ve desteklemek için dışarıdan destek kullanılacaktır.

Okul, öğrencilerin ihtiyaçlarına uygun olarak çevrimiçi güvenliği geliştirmek için akran eğitimi uygulayacaktır.

## **PERSONELİN KATILIMI VE EĞİTİMİ**

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 izlenebileceğinin farkında olacaktır. 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) olarak sağlanacaktır.

Çalışanların tüm üyeleri, çevrimiçi davranışlarının okuldaki rolü ve itibarını etkileyebileceğinin farkına varacaktır.

BİT kullanımını izleme sorumluluğu taşıyan personel, sorunları ve endişeleri okul idaresine bildirecektir.

Okul, tüm paydaşların yaşlarına ve yeteneklerine göre kullanması gereken yararlı çevrimiçi araçları vurgulamaktadır.



## **EBEVEYNLERİN KATILIMI VE EĞİTİMİ**

Bağlıca Anadolu Lisesi, çocukların internetin ve dijital teknolojinin güvenilir ve sorumlu kullanıcıları olabilmesi için ana-babaların önemli bir role sahip olduklarını kabul eder.

Ebeveynlerin dikkatleri, okul çevrimiçi güvenlik (e-Güvenlik) politikasına ve beklentilerine yönelecektir.

Okulumuzun bir parçası olarak ebeveynlerin çevrimiçi güvenlik bilgilerini okumaları istenecektir.

Ebeveynler, Kabul Edilebilir Kullanım Politikalarını (AUP)'u okumaya ve çocukları ile etkilerini tartışmaya teşvik edilecektir.

Çevrimiçi güvenlik konusundaki "ebeveynler için bilgi ve rehberlik", ebeveynlere çeşitli biçimlerde sunulacaktır.

Ebeveynlerin, çevrimiçi olarak çocukları için olumlu davranışları rol modellemeleri teşvik edilecektir.

## **ÇEVİRİMİÇİ OLAYLARA VE KORUMA SORUNLARINA YANIT VERME**

Okulun tüm üyeleri, sakıncalı mesajlaşma, çevrimiçi/siber zorbalık vb. dâhil olmak üzere karşılaşılabilecek çevrimiçi risklerin çeşitliliğinden haberdar edilecektir. Bu, öğrencilere yönelik personel eğitimi ve eğitim yaklaşımları içerisinde vurgulanacaktır.

Okulun tüm üyeleri, filtreleme, sakıncalı mesajlaşma, siber zorbalık, yasadışı içerik ihlali vb. gibi çevrimiçi güvenlik (e-Güvenlik) endişelerini bildirme prosedürü hakkında bilgilendirilecektir.

Çevrimiçi/siber zorbalık ile ilgili şikâyetler, okulun zorbalık karşıtı politikası ve prosedürü kapsamında ele alınacak

İnternet'in yanlış kullanımı ile ilgili şikâyetler, okulun şikâyet prosedürleri kapsamında ele alınacaktır.

Personelin yanlış kullanımı ile ilgili herhangi bir şikâyet okul müdürüne yönlendirilecektir

Okul şikâyet prosedürü öğrencilere, velilere ve personele bildirilecektir.

Şikâyet ve ihbar prosedürü personele bildirilecektir.

Okulun tüm üyeleri, gizliliğin öneminden ve endişeleri bildirmek için resmi okul usullerine uyma ihtiyacından haberdar olmalıdırlar.

Okulun tüm üyelerine, okul camiasının herhangi bir diğer üyesine zarar vermek, sıkıntı yaşamak veya suç oluşturan herhangi bir içerik, yorum, resim veya video yayımlamamanın önemini hatırlatılacaktır.

Okul, çevrimiçi güvenlik (e-güvenlik) olaylarını, uygun olduğunda, okul disiplini/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 gerekir.