

GÖRÜKLE DUMLUPINAR İLKOKULU  
MÜDÜRLÜĞÜ  
E-GÜVENLİK OKUL POLİTİKASI VE  
KURALLARI

BURSA - NİLÜFER

2016

## AMAÇ:

- Görükle Dumlupınar İlkokulu, e-güvenlik çalışmaları ile internet, bilgisayar, dizüstü 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.

## Bu Politikada;

**Kurum:** Görükle Dumlupınar İlkokulu

**Yönetim:** Okul idaresi (müdür/müdür yardımcısı)

**AR-GE BİRİMİ:** Asuman YAĞMUROĞLU, Ramazan CALAYIR, Gonca Sevda ERDEN, Ercan ÜRKMEZ

**Personel:** öğretmenler ve yardımcı hizmetliler

**Çocuklar:** öğrenciler

**Paydaş:** Veliler, ziyaretçiler, okul adına hizmet veren diğer kişiler olarak tanımlanmaktadır.

**Üye:** Yönetim, personel, öğrenci ve diğer paydaşları kapsamaktadır.

Bu politika, yönetim, personel, çocuklar ve paydaşlar için geçerlidir.

Bu politika, internet erişimi ve kişisel cihazlar da dahil olmak üzere tüm bilgi iletişim cihazlarının kullanımı için geçerlidir.

## SORUMLULUKLAR:

- E-güvenlik politikalarının gelişmesine katkıda bulunmak.
- Olumlu öğrenme aşamasında mesleki gelişim için sorumluluk almak.
- Okulu ve içerisindeki kişileri korumak için e-güvenlik konusunda sorumluluk almak.
- Teknolojiyi güvenli ve sorumlu kullanmak.
- Zarar görülmesi durumunda tehlikeyi gözlemleyip ilgili birimlere iletmek.

### -Personelin Sorumlulukları:

1. Çevrimiçi güvenlik politikalarının geliştirilmesine katkıda bulunmak.
2. Kabul Edilebilir Kullanım Politikalarını (AUP) okumak ve onlara bağlı kalmak.
3. Okul sistemlerinin ve verilerin güvenliğinden sorumlu olmak.
4. Bir dizi farklı çevrimiçi güvenlik konusundaki farkındalığa sahip olmak ve onların bakımında çocuklarla nasıl ilişkili olabileceklerini bilmek.
5. Yeni ve gelişmekte olan teknolojiler kullanıldığında iyi uygulamaları öğrenmek ve hayata geçirmek.
6. Müfredatımız ile çevrimiçi güvenlik eğitimi ilişkilendirmek.
7. Okul güvenlik politikalarını ve prosedürlerini takip etmek, endişe duyan bireylerin belirleyerek uygun önlemleri almak.
8. Çevrimiçi güvenlik konularında, dahili ve harici olarak, uygun destekleri sağlamak.
9. Kişisel ve kişisel teknoloji kullanımlarında, hem açık hem de kapalı alanda profesyonel bir davranış sergilemek.
10. Olumlu öğrenme fırsatlarına vurgu yapmak.
11. Bu alanda mesleki gelişim için kişisel sorumluluk almak.

### -Çocukların Sorumlulukları:

1. Çevrimiçi güvenlik politikalarının geliştirilmesine katkıda bulunmak.
2. Okulun Kabul Edilebilir Kullanım Politikalarını (AUP) okumak ve onlara bağlı kalmak.
3. Çevrim içi ve çevrimdışı başkalarının hislerine ve haklarına saygı duymak.
4. Güvenilir bir yetişkinden yardım istemek ve çevrimiçi güvenlik sorunlarıyla karşılaşan diğer kişileri desteklemek.

5. Kendilerini ve başkalarını çevrimiçi olarak korumak için sorumluluk almak.
6. Yeni ve gelişmekte olan teknolojilerin getirdiği fırsatlar ve risklerle ilgili olarak kendi bilinci ve öğrenimlerinden sorumlu olmak.
7. Teknolojiyi kullanmanın kişisel risklerini değerlendirmek ve bu riskleri sınırlamak için güvenli ve sorumluluk sahibi davranmak.

#### -Ebeveynlerin Sorumlulukları:

1. Okul Kabul Edilebilir Kullanım Politikalarını (AUP) okumak ve bağlı kalmak.
2. Çocuklarını bu politikaya bağlı kalmasını sağlamak.
3. Çocuklarıyla çevrimiçi güvenlik konularını tartışmak.
4. Okulun çevrimiçi güvenlik yaklaşımlarını desteklemek.
5. Evde uygun güvenli çevrimiçi davranışları pekiştirmek.
6. Teknoloji ve sosyal medyanın güvenli ve uygun kullanımını modellemek.
7. Davranışlarında, çocuğun çevrimiçi olarak zarar görme tehlikesi altında olduğunu gösteren değişiklikleri belirlemek.
8. Okul veya diğer uygun kurumlardan, kendileri veya çocukları çevrimiçi problem veya sorunlarla karşılaşırsa yardım veya destek istemek.
9. Okulun çevrimiçi güvenlik politikalarının oluşturulmasına katkıda bulunmak.
10. Öğrenme platformları ve diğer ağ kaynakları gibi okul sistemlerini güvenli ve uygun bir şekilde kullanmak.
11. Yeni ve gelişmekte olan teknolojilerin getirdiği fırsatlar ve risklerle ilgili olarak kendi bilinci ve öğrenimlerinden sorumlu olmak.

**OKUL WEB SİTESİ:** <https://gorukledumlupinarilkokulu.meb.k12.tr/tema/index.php>

- Görükle Dumlupınar İlkokulu olarak web sitemizde okulumuzun adres, telefon, fax ve e posta adres bilgileri bulunmaktadır.
- Sitemizde yayınlanan tüm içerikler okul müdürümüzün 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 yayınlanmaktadır.
- Öğrenci çalışmaları ebeveynlerinin izniyle yayınlanacaktır.
- Personel veya öğrencilerin kişisel bilgileri yayınlanmayacaktır.
- Okul web sitesinin yönetici hesabı, uygun bir şekilde güçlü şifreyle şifrelenerek korunacaktır.
- 

#### 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.

### 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.

### 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 kullanımı konusunda bilgilendirilmiştir.
- Tüm okul cihazlarımız virüs korumalıdır.
- E-güvenlik ve siber zorbalık konuları belli derslerimizin yıllık planlarına dahil edilmiş olup, bu konularda yıl içinde öğrencilere bilgi aktarımı devam etmektedir.
- Çevrimiçi materyaller öğretme ve öğrenmenin önemli bir parçası olup müfredat içinde aktif olarak kullanılmaktadır.
- 09 Şubat güvenli internet günü okulumuzda kutlanmaktadır.
- Okulumuz 5651 yasasına uygun güvenlik prosedürlerini tamamen uygulamaktadır.

### 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.

### 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 öğrencileri, velilerini aramaları gerektiği durumlarda okula ait olan telefonları bir okul idarecisi gözetiminde kullanabilirler.
- Velilerimiz okul saatleri içerisinde öğrencileriyle görüşme yapmamaları gerektiği konusunda bilgilendirilirler. Eğer zorunlu haller var ise okul yönetiminden izin alarak görüşme yapmaları sağlanmalıdır.
- Çalışanlar (öğretmen, idareci, personel vb) kişisel cep telefonlarını ders saatlerinde sessize alarak ya da kapatarak görevlerine devam etmelidir.
- 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.

## GÜVENLİK EĞİTİMİ:

- Öğrenciler için e-güvenlik müfredatı ilgili derslerin yıllık planlarına eklenerek öğrenciler bu konularda bilgilendirilir.
- Tüm kullanıcıların internet kullanımları bilgi işlem birimi tarafından takip edilmektedir. Bu bilgi tüm kullanıcılara iletilmiştir.
- Öğrencilerimizin ihtiyaçları doğrultusunda çevrimiçi güvenliği geliştirmek için rehberlik öğretmenleri ekran eğitimi uygulamaktadır.
- Çevrimiçi güvenlik politikası tüm çalışanlarımıza resmi olarak duyurulacaktır.
- 09 Şubat güvenli internet günü okulumuzda kutlanmaktadır. Bugüne yönelik okul koridorları ve sınıflarda pano çalışmalarımız ve sosyal medya paylaşımlarımız olur.

## Çocukların ve gençlerin katılımı ve 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) / BİT programlarına dahil edilecek ve hem güvenli okul hem de evde kullanımını kapsayacaktır.
- Kabul Edilebilir Kullanım beklentileri ve Posterler, İnternet erişimi olan tüm odalarda yayınlanacaktır.
- İnternetin ve teknolojinin güvenli kullanımı müfredatta işlenecektir.
- Okul, öğrencilerin teknolojiyi olumlu şekilde kullandıklarını ödüllendirecektir.
- Okul, öğrencilerin ihtiyaçlarına uygun olarak çevrimiçi güvenliği geliştirmek için ekran eğitimi uygulayacaktır.

## Personelin katılımı ve 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, 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 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.
- Filtreleme sistemlerini yönetme veya BİT kullanımını izleme sorumluluğu taşıyan personel, okul yönetimi tarafından denetlenecek ve sorunları veya endişeleri bildirmek için açık prosedürlere sahip olacaktır.
- Personele şifrelerini hiçbir şekilde bilgisayarın görünen bir yüzüne yazılmaması uyarısı yapılacak.
- Okul, çalışanların öğrencilerin yaşlarına ve yeteneklerine göre kullanması gereken yararlı çevrimiçi araçları vurgulayacaktır.

## Ebeveynlerin katılımı ve eğitimi

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

- Ebeveynler için, okul web sitesinde okul çevrimiçi güvenlik (e-Güvenlik) politikasına, beklentilerine ve diğer e güvenlik konuları hakkında bilgilere yer verilecektir.
- Okullarımızın bir parçası olarak ebeveynlerin çevrimiçi güvenlik bilgilerini okumaları istenecektir.
- Ebeveynler, Okulun Kabul Edilebilir Kullanım Politikasını okumaya ve çocuklarıyla etkilerini tartışmaya teşvik edilecektir.
- Çevrimiçi güvenlik konusunda ebeveynler için bilgi ve rehberlik, ebeveynlere çeşitli biçimlerde sunulacaktır.
- Ebeveynlerin, çevrimiçi olarak çocukları için olumlu davranışlarla rol model olmaları teşvik edilecektir.

#### ÇEVİRİMİÇİ OLAYLAR VE KORUMA:

- Okulumuzun tüm üyeleri çevrimiçi riskler konusunda bilgilendirilecektir. Eğitimler yapıp içerikler açıklanacaktır.
- Okulumuzda yasadışı içerik, güvenlik ihlali, siber zorbalık, cinsel içerikli mesajlaşma, çocuk istismarı, kişisel bilgi güvenliği gibi konularda bilgilendirme çalışmaları yapılmaktadır.
- 09 Şubat güvenli internet günü kutlanmaktadır.
- Okulumuzda internet, bilgi teknolojileri ve ekipmanlarının yanlış kullanımı ile ilgili tüm şikâyetler okul müdürüne bildirilecektir.
- Okulumuzun tüm üyeleri gizlilik ve güvenlik endişelerini ortadan kaldırmak için resmi okul kurallarına uygun şekilde davranışları hususunda bilgilendirilir.
- Sorunların çözümünde çalışanlar (öğretmen, idareci, personel vb), veliler ve öğrenciler okul ile birlikte hareket etmelidir.

AR-GE BİRİMİ, e-güvenlik birimi olarak öğretmenler kurulu kararı ile görevlendirilmiştir.

Asuman YAĞMUR OĞLU  
Rehber Öğretmen

Gonca Sevdâ ERDEN  
İngilizce Öğretmeni

Ercan ÜRKİMEZ  
Şifre Öğretmeni

Ramazan CALAYIR  
Müdür Yardımcısı

Abdullah URGAN  
Okul Müdürü

## GÖRÜKLE DUMLUPINAR PRIMARY SCHOOL ACCEPTABLE USE POLICY (AUP)

This document has been prepared about how and by whom the information and information technologies to be used in our school will be used and what to pay attention to.

Our School's Acceptable Use Policy covers the safety and use of everyone.

This policy applies to all;

Cell Phones

Tablet Computers

Laptop Computers

Desktop Computers for Personal and Public Use

Includes cameras and all the cameras that take pictures.

Users must use all these information tools according to our school's usage policy. In our school, realized with the above-mentioned information devices; E-mail, internet, voice and mobile communication, receiving and sending data over the internet or network, making publications that concern the institution at school or outside the school, and sharing texts, pictures and videos on web pages must be carried out within the usage policy.

This policy covers all Görükle Dumlupinar Primary School administrators, teachers, staff, students, parents and all our stakeholders, which are also specified in the school and security policy. This policy is valid for all data about Görükle Dumlupinar Primary School.

### GENERAL RULES AND LIMITATIONS

All users must obtain their computer user name and password with an official letter from the administration. Individuals cannot give their username and password for someone else to use.

Users cannot log in as an administrator on public computers.

Individuals open and use desktop computers and interactive boards allocated to them in our school with their User IDs.

Individuals and users cannot change system settings in computer and information systems. They cannot install software. All computing devices are encrypted for changing system settings and installing software. Our school vice principal is responsible for this issue. Consult him for any changes.

Individuals cannot use data that they are not authorized to use or access.

Individuals cannot use computers that are not authorized

Only people in the administration can operate on the computers in the administrative rooms of our school.

Teachers can log in with the user name and password given to them on the desktop computer and interactive whiteboard in the teachers' room and classrooms.

In our school computer systems, external flash disks, cd rooms, etc. The use of data storage and transfer equipment can be provided with the permission of the administrator.

Internet and e-mail usage in our school is provided by using official e-mail only for administrators.

Opening personal e-mails on corporate computers is subject to legal permission from the administration, clicking link links is prohibited. All individuals are responsible for their actions on the internet and e-mail system.

It is forbidden for individuals to access the school's internet network systems with their mobile phones. For educational use, permission and password must be obtained from the administration beforehand.

Individuals cannot take pictures and videos and post them on the Internet using mobile phones and other technologies without permission. For images to be taken for educational purposes, permission must be obtained from the administration beforehand.

If there is any information and news that you want to be published on our school website, first examine our article review board and submit it to our school website setup. If our board deems appropriate, your news will be published on our website.

Students are forbidden to bring personal cell phones, tablets, computers, etc. to our school. You can apply to our school e safety commission in case of any problem.

AR-GE Unit is assigned as the eSafety unit by the decision of the teachers board.

Asuman YAĞMURUOĞLU

Rehber Öğretmen

Gonca Sevda ERDEN

English Teacher

Ercan ÜRKMEZ

Classroom Teacher

Ramazan CALAYIR  
Asistand Director

Abdullah URGAN  
School Manager

BURSA - NİLÜFER

2016