OKULUN DİJİTAL GÜVENLİK POLİTİKASI

1. Giriş

Bu belge, Gemlik Anadolu İmam Hatip Lisesinin dijital güvenlik standartlarını ve kurallarını belirler. Okulumuz, öğrenci, öğretmen ve personelin dijital ortamda güvenliğini sağlamak için belirli politikalar uygulamaktadır.

2. Amaç

Bu politikanın amacı:

- Okul ağının, dijital kaynakların ve internet kullanımının güvenli olmasını sağlamak,
- Siber zorbalık, veri hırsızlığı ve kötü amaçlı yazılımlara karşı önlemler almak,
- Öğrencilerin ve çalışanların kişisel verilerini korumak,
- Okulun teknolojik altyapısının verimli ve güvenli şekilde kullanılmasını sağlamaktır.

3. Kapsam

Bu politika, Gemlik Anadolu İmam Hatip Lisesi bünyesindeki tüm öğrencileri, öğretmenleri, idari personeli ve okul internetini veya cihazlarını kullanan ziyaretçileri kapsar.

4. Dijital Güvenlik İlkeleri

4.1. Genel Kurallar

- Okulun internet ağı, yalnızca eğitim amaçlı kullanılmalıdır.
- Bilgisayar laboratuvarları ve akıllı tahtalar gibi dijital cihazlar, yalnızca ders kapsamında kullanılmalıdır.
- Güçlü ve düzenli olarak değiştirilen şifreler kullanılmalıdır.
- Öğrenci ve personel hesapları, yetkisiz kişilerle paylaşılmamalıdır.
- Kişisel bilgiler, sosyal medyada veya bilinmeyen platformlarda paylaşılmamalıdır.

4.2. İnternet Kullanımı

- Öğrenciler, okulun internet ağında uygunsuz veya zararlı içeriklere erişmemelidir.
- Öğretmenler ve öğrenciler, yalnızca güvenilir ve lisanslı eğitim materyallerini kullanmalıdır.
- Okulun interneti, siber saldırılara karşı güvenlik duvarları ile korunmaktadır.
- VPN, proxy veya benzeri araçlarla yasaklı sitelere erişim sağlamak yasaktır.

4.3. Kişisel Verilerin Korunması

- Öğrencilerin ve çalışanların kişisel bilgileri, üçüncü kişilerle paylaşılmamalıdır.
- Veliler, çocuklarının dijital ortamlardaki güvenliği konusunda bilgilendirilmelidir.
- Okul e-posta adresleri, yalnızca akademik amaçlarla kullanılmalıdır.

- Sosyal medya kullanımında okulun ve öğrencilerin güvenliği göz önünde bulundurulmalıdır.

4.4. Dijital Cihaz ve Yazılım Kullanımı

- Okul tarafından sağlanan bilgisayarlar ve tabletler, eğitim dışı amaçlarla kullanılmamalıdır.
- Öğrenciler, kendi cihazlarını okula getirmeden önce okul yönetiminden izin almalıdır.
- Yazılım ve uygulamalar, yalnızca okulun belirlediği güvenilir kaynaklardan indirilmelidir.
- Okul sistemlerine yetkisiz erişim sağlamak kesinlikle yasaktır.

5. Siber Zorbalık ve Etik Kurallar

- Başkalarını rahatsız eden, tehdit eden veya aşağılayan mesajlar paylaşmak yasaktır.
- Siber zorbalık tespit edildiğinde, rehberlik servisi ve okul yönetimi bilgilendirilmelidir.
- Dijital ortamda saygılı ve etik kurallar çerçevesinde iletişim kurulmalıdır.

6. İhlal Durumunda Alınacak Önlemler

- Bu politikaya uymayan öğrenciler ve çalışanlar hakkında disiplin yönetmeliği uygulanacaktır.
- Kişisel verilerin izinsiz paylaşılması, ilgili yasal düzenlemelere göre değerlendirilir.
- Siber saldırı veya güvenlik ihlali durumunda, okul BT ekibi derhal müdahale eder ve gerekli yasal işlemler başlatılır.

7. Politikanın Güncellenmesi

Bu belge, yılda en az bir kez gözden geçirilerek güncellenir. Değişiklikler okul yönetimi tarafından duyurulacaktır.

8. Yetkili Kişiler ve İletişim

Dijital güvenlikle ilgili sorular ve bildirimler için aşağıdaki yetkililerle iletişime geçebilirsiniz:

- varlık.sedat@gmail.com
- 0224 513 1728

Gemlik Anadolu İmam Hatip Lisesi Yönetimi
01.01.2025

Bu belge, öğrenciler, veliler, öğretmenler ve personel için dijital güvenlik konusunda net kurallar koyarak bilinçli ve güvenli internet kullanımını teşvik eder. Ayrıca, okulun dijital sistemlerini kötüye kullanıma karşı korur.

BİLGİ GÜVENLİĞİ POLİTİKASI

 Yayın Tarihi: 01.01.2025
 Hazırlayan: Gemlik Anadolu İmam Hatip Lisesi Yönetimi

---

1. Amaç

Bu belgenin amacı, Gemlik Anadolu İmam Hatip Lisesi bünyesindeki tüm öğrencilerin, öğretmenlerin ve personelin bilgi güvenliğini sağlamak için alınacak önlemleri ve uyulması gereken kuralları belirlemektir.

2. Kapsam

Bu politika, Gemlik Anadolu İmam Hatip Lisesi'nda bulunan tüm dijital ve fiziksel bilgi sistemlerini, öğrencilerin ve personelin kişisel verilerini, okul ağına bağlanan tüm cihazları ve internet kullanımını kapsar.

---

3. Bilgi Güvenliği İlkeleri

3.1. Genel İlkeler

✅Okulun tüm bilgi sistemleri yalnızca eğitim ve idari işler için kullanılmalıdır.
✅Kişisel veriler, yetkisiz erişime karşı korunmalıdır.
✅Kullanıcı hesapları ve şifreler gizli tutulmalıdır.
✅Dijital ortamlarda paylaşılan bilgilerin gizliliği korunmalıdır.

3.2. Yetkisiz Erişimin Önlenmesi

 Öğrenciler ve personel, yalnızca yetkilendirildikleri sistemlere erişim sağlayabilir.
 Okul bilgisayarları ve veri tabanları, güçlü şifreleme yöntemleri ile korunmalıdır.
 Yetkisiz kişilerin okul sistemlerine erişimi engellenmelidir.
 Okulun internet ağı, güvenlik duvarları ve antivirüs yazılımları ile korunmalıdır.

3.3. Şifre ve Hesap Güvenliği

 Okul e-posta hesapları ve öğrenci/öğretmen portalları güçlü şifreler ile korunmalıdır.
 Kullanıcılar, belirli aralıklarla şifrelerini değiştirmelidir.
 Şifreler başkalarıyla paylaşılmamalıdır.
 Bilinmeyen cihazlarda otomatik oturum açma özelliği kullanılmamalıdır.

3.4. Kişisel Verilerin Korunması

 KVKK (Kişisel Verileri Koruma Kanunu) kapsamında öğrencilerin, öğretmenlerin ve velilerin kişisel bilgileri korunmalıdır.
 Öğrenci ve öğretmen bilgileri yalnızca ilgili kişiler tarafından görüntülenebilir.
 Okul sistemlerinde yer alan veriler, düzenli olarak yedeklenmelidir.
 Kişisel veriler, yalnızca yasal zorunluluklar çerçevesinde paylaşılmalıdır.

3.5. Fiziksel Güvenlik Önlemleri

 Bilgi işlem odaları yetkisiz girişlere karşı kilitlenmeli ve yalnızca yetkili personel erişim sağlamalıdır.
 Dersliklerde ve laboratuvarlarda kullanılan bilgisayarlar gözetimsiz bırakılmamalıdır.
 Yazılı belgeler ve dokümanlar, kilitli dolaplarda muhafaza edilmelidir.

---

4. Bilgi Güvenliği İçin Alınacak Önlemler

4.1. Teknik Önlemler
✔ Okul ağı ve bilgisayar sistemleri güvenlik duvarları ile korunmalıdır.
✔ Antivirüs ve güvenlik yazılımları düzenli olarak güncellenmelidir.
✔ Güvenli internet kullanımı için filtreleme sistemleri kullanılmalıdır.
✔ Okul veri tabanları düzenli olarak yedeklenmelidir.
✔ USB bellek, harici disk gibi depolama aygıtları kontrolsüz şekilde kullanılmamalıdır.

4.2. Kullanıcı Bilinci ve Eğitim
✔ Öğrenciler ve öğretmenler, siber güvenlik konusunda düzenli olarak bilgilendirilmelidir.
✔ Bilgi güvenliği politikaları, öğrencilere ve velilere duyurulmalıdır.
✔ Sosyal medya ve internet kullanımıyla ilgili bilinçlendirme seminerleri düzenlenmelidir.

4.3. İhlal Tespiti ve Müdahale Prosedürleri
✔ Şüpheli bir güvenlik ihlali tespit edildiğinde, BT yöneticisi ve okul yönetimi bilgilendirilmelidir.
✔ Siber saldırılar veya veri sızıntıları durumunda acil müdahale planı uygulanmalıdır.
✔ Yetkisiz erişimler tespit edilirse, kullanıcı hesapları geçici olarak askıya alınmalıdır.

4.4. Sosyal Medya ve İnternet Kullanımı
✔ Öğrenciler, sosyal medya hesaplarını bilinçli ve güvenli bir şekilde kullanmalıdır.
✔ Okul adı ve logosu, izinsiz şekilde internette paylaşılmamalıdır.
✔ Siber zorbalık ve kötüye kullanım durumlarında, rehberlik servisi ve okul yönetimi bilgilendirilmelidir.

---

5. Politikanın Uygulanması ve Denetimi

 Okul yönetimi ve BT birimi, bu politikaların uygulanmasını denetlemekle sorumludur.
 Politika yılda en az bir kez gözden geçirilerek güncellenir.
 Kullanıcılar, bilgi güvenliği kurallarına uymadıkları takdirde disiplin yönetmeliğine tabi tutulacaktır.

---

6. Yetkili Kişiler ve İletişim

Bilgi Güvenliği Sorumlusu: [Ad Soyad]
 E-Posta: varlik.sedat@gmail.com
 Telefon: 0224 513 1728

Gemlik Anadolu İmam Hatip Lisesi Yönetimi
 Tarih: 01.01.2025

Sonuç

Bu politika, okulun **bilgi varlıklarını korumayı, veri güvenliğini sağlamayı ve tüm öğrenciler ile personelin bilinçli bir şekilde dijital ortamları kullanmasını** amaçlamaktadır. **Tüm öğrenciler, öğretmenler ve veliler bu politikaya uymakla yükümlüdür.**

Bu belge, **okul internet sitesine, öğrenci portalına veya e-posta ile tüm kullanıcılara** duyurulabilir.

ÖĞRENCİLER İÇİN İNTERNET KULLANIM KURALLARI

 Yayın Tarihi: 01.01.2025
 Hazırlayan: Gemlik Anadolu İmam Hatip Lisesi Yönetimi

---

1. Amaç

Bu belge, Gemlik Anadolu İmam Hatip Lisesi öğrencilerinin okul içinde ve dışında interneti **güvenli, bilinçli ve etik kurallar çerçevesinde** kullanmalarını sağlamak amacıyla hazırlanmıştır.

---

2. Genel Kurallar

✅İnternet, eğitim amaçlı kullanılmalıdır.
✅Kişisel bilgilerin gizliliği korunmalıdır.
✅Saygılı ve etik bir dil kullanılmalıdır.
✅Yasalar ve okul kurallarına uyulmalıdır.
✅Güvenilir kaynaklardan bilgi alınmalıdır.

---

3. Ders İçinde İnternet Kullanımı

 Ders sırasında internet sadece öğretmen yönlendirmesiyle kullanılmalıdır.
 Öğrenciler, öğretmenin belirttiği eğitim materyallerine erişmelidir.
 Sosyal medya, oyun ve eğlence sitelerine giriş yasaktır.
 Okulun dijital eğitim platformları dışındaki siteler izin alınmadan ziyaret edilmemelidir.
 Öğrenciler, okul bilgisayarlarında veya tabletlerinde yalnızca okul tarafından onaylanan yazılımları kullanmalıdır.

---

4. Ders Dışı İnternet Kullanımı

 Öğrenciler, ders dışında interneti güvenli ve bilinçli bir şekilde kullanmalıdır.
 Sosyal medya platformlarında başkalarına saygılı davranılmalı, siber zorbalık yapılmamalıdır.
 Güvenli ve lisanslı içerikler tercih edilmelidir.
 Kişisel bilgilerin (adres, telefon numarası, şifre vb.) paylaşılmaması gerekmektedir.
 Tanımadığınız kişilerle çevrim içi iletişim kurulurken dikkatli olunmalıdır.
 Zararlı içeriklere karşı dikkatli olunmalı, şüpheli siteler ziyaret edilmemelidir.

---

5. Okul İnternet Ağı Kullanım Kuralları

 Okul Wi-Fi ağı sadece akademik çalışmalar için kullanılmalıdır.
 VPN, proxy veya benzeri araçlarla erişim sağlamak yasaktır.
 Bilinmeyen ve güvenilmeyen bağlantılara tıklanmamalıdır.
 Okul ağı üzerinden büyük boyutlu dosyalar (film, oyun vb.) indirilmemelidir.
 Başkasının hesabını kullanmak veya yetkisiz giriş yapmak kesinlikle yasaktır.

---

6. Sosyal Medya ve Dijital Kimlik Kullanımı

 Sosyal medyada okulun adı, logosu veya öğrenci bilgileri izinsiz paylaşılmamalıdır.
 Başkalarının kişisel bilgileri veya fotoğrafları, izinsiz olarak paylaşılmamalıdır.
 Siber zorbalık, hakaret, tehdit gibi davranışlarda bulunulmamalıdır.
 Sahte hesaplar açmak ve başkalarının kimliğini taklit etmek yasaktır.

---

7. Güvenli İnternet Kullanımı İçin Öneriler

 Güçlü şifreler oluşturun ve düzenli olarak değiştirin.
 Antivirüs yazılımlarını güncel tutun.
 Şüpheli e-postalara ve bağlantılara tıklamayın.
 İnternette paylaştığınız bilgilerin kalıcı olabileceğini unutmayın.
 Şüpheli durumları öğretmenlerinize veya okul yönetimine bildirin.

---

8. Kurallara Uyulmaması Durumunda Alınacak Önlemler

 Bu kurallara uymayan öğrenciler hakkında disiplin yönetmeliği uygulanacaktır.
 Yetkisiz erişim, zararlı içerik kullanımı veya siber zorbalık durumlarında veli bilgilendirilecek ve gerekli hukuki süreç başlatılacaktır.
 Öğrencinin internet erişimi geçici olarak kısıtlanabilir.

---

9. Yetkili Kişiler ve İletişim

Dijital Güvenlik Sorumlusu:
 E-Posta: varlik.sedat@gmail.com
 Telefon: 0224 513 1728

Gemlik Anadolu İmam Hatip Lisesi Yönetimi
 Tarih: 01.01.2025

Bu belge, öğrencilerin **internet ortamında güvenli, sorumlu ve bilinçli hareket etmelerini sağlamak** amacıyla oluşturulmuştur. **Tüm öğrenciler, bu kurallara uymakla yükümlüdür.**

VELİLER İÇİN E-GÜVENLİK BİLGİLENDİRME KILAVUZU

 Yayın Tarihi: 01.01.2025
 Belge No: [Belge Numarası]
 Hazırlayan: Gemlik Anadolu İmam Hatip Lisesi Yönetimi

---

1. Giriş

Bu kılavuz, velilerin çocuklarının **dijital dünyada güvenliğini sağlamak** ve **siber risklerden korunmalarına yardımcı olmak** amacıyla hazırlanmıştır. Günümüzde internet, eğitim ve bilgiye erişim açısından büyük avantajlar sunarken; bilinçli kullanılmadığında **siber zorbalık, kişisel veri güvenliği ihlalleri ve zararlı içeriklerle karşılaşma riski** taşır.

Bu kılavuzda **e-güvenlik konusunda alınabilecek önlemler ve çocukların interneti bilinçli kullanmaları için yapılması gerekenler** açıklanmıştır.

---

2. Çocukların Güvenli İnternet Kullanımı İçin Temel Kurallar

 Güvenilir ve yaşlarına uygun içerikleri kullanmalarını sağlayın.
 İnternet kullanımını belli bir süreyle sınırlandırın.
 Kişisel bilgilerini paylaşmamaları gerektiğini öğretin.
 Tanımadıkları kişilerle çevrim içi iletişim kurarken dikkatli olmalarını hatırlatın.
 Sosyal medya hesaplarının gizlilik ayarlarını düzenleyin.
 Onlara internetin kalıcı olduğunu ve paylaştıkları her şeyin iz bırakabileceğini anlatın.

---

3. Siber Tehditler ve Alınacak Önlemler

3.1. Siber Zorbalık

❌Tehdit, hakaret, küçük düşürücü mesajlar ve siber zorbalık içeren davranışlar, çocukların psikolojik sağlığını olumsuz etkileyebilir.

✅Çözüm:
✔ Çocuğunuzun çevrim içi ortamlarda karşılaştığı olumsuz durumları sizinle paylaşmasını sağlayın.

✔ Sosyal medya ve mesajlaşma uygulamalarında tanımadıkları kişilerle iletişim kurmamaları gerektiğini anlatın.
✔ Siber zorbalık mağduru olmaları durumunda, delilleri saklayarak okul yönetimi veya ilgili yasal mercilere başvurun.

3.2. Kişisel Veri Güvenliği

✖Çocuklar, isim, adres, okul bilgileri, telefon numarası gibi kişisel bilgilerini bilinçsizce paylaşabilirler.

✅Çözüm:
✔ Çocuğunuza, tanımadığı kişilerle kişisel bilgilerini paylaşmaması gerektiğini anlatın.
✔ Sosyal medya hesaplarının gizlilik ayarlarını en güvenli hale getirin.
✔ Okulun ve güvenilir eğitim platformlarının dışındaki yabancı sitelere kişisel bilgi girmemesini sağlayın.

3.3. Zararlı İçerik ve Dolandırıcılıklar

✖Bazı internet siteleri ve uygulamalar, çocuklara uygun olmayan içerikler barındırabilir. Ayrıca, dolandırıcılık amacıyla sahte mesajlar veya bağlantılar da paylaşılabilir.

✅Çözüm:
✔ Çocuğunuzun yaşına uygun web sitelerine ve uygulamalara eriştiğinden emin olun.
✔ **Aile koruma filtreleri ve ebeveyn denetim programları** kullanın.
✔ Şüpheli e-postalara, mesajlara veya reklamlara tıklamamaları gerektiğini öğretin.
✔ Çevrim içi alışverişlerde dikkatli olun ve çocuğunuzun kredi kartı bilgilerini paylaşmadığından emin olun.

---

4. Güvenli Sosyal Medya Kullanımı İçin Öneriler

□ Çocuklarınızın sosyal medya hesaplarının gizlilik ayarlarını kontrol edin.
□ Kimlerle arkadaş olduklarını gözden geçirin.
□ İnternette yazdıkları veya paylaştıkları içeriklerin gelecekte etkili olabileceğini anlatın.
□ Başkalarının bilgilerini izinsiz paylaşmamaları gerektiğini öğretin.
□ Canlı yayın yaparken konum veya kişisel bilgilerin paylaşılmaması gerektiğini vurgulayın.

---

5. Ebeveyn Denetimi ve Dijital Rehberlik

 Aile içi dijital kullanım kuralları belirleyin ve tüm aile bireyleri bu kurallara uysun.
 Çocuklarınızın hangi sitelere girdiğini, kimlerle iletişim kurduğunu bilin.
 Okulun sağladığı dijital platformların güvenilirliğini kullanın ve okul ile iş birliği içinde olun.
 Bilgi güvenliği ve siber tehditler hakkında çocuğunuzla düzenli konuşun.

5.1. Ebeveyn Kontrol Araçları

✅Google Family Link, Microsoft Family Safety, Apple Screen Time gibi ebeveyn kontrol yazılımlarını kullanabilirsiniz.
✅YouTube Kids gibi çocuk dostu içerik sunan platformları tercih edin.
✅İnternet kullanımı için zaman sınırlamaları koyun ve belirli saatlerde cihaz kullanımına izin verin.

---

6. Acil Durumlarda Ne Yapılmalı?

 Çocuğunuz siber zorbalık, dolandırıcılık veya uygunsuz içerikle karşılaşırsa:
 Öncelikle sakin olun ve çocuğunuzu suçlamayın.
 İlgili mesajları, e-postaları veya ekran görüntülerini kaydedin.
 Okul yönetimine veya rehberlik servisine bilgi verin.
 Gerekirse Siber Suçlarla Mücadele Birimi'ne veya BTK'ya (Bilgi Teknolojileri ve İletişim Kurumu) başvurun.

---

7. Okul ve Veli İş Birliği

 Okul olarak **velilerin bilinçlendirilmesi ve öğrencilerin güvenliği için** aşağıdaki adımları atıyoruz:
 Düzenli e-güvenlik seminerleri düzenliyoruz.
 Okul içi internet güvenliği politikalarını uyguluyoruz.
 Öğrencilerin güvenli eğitim platformları kullanmalarını sağlıyoruz.

 Veliler olarak siz de çocuklarınızı dijital dünyada güvende tutmak için bizlerle iş birliği içinde olun!

---

8. İletişim Bilgileri

Bilgi Güvenliği Sorumlusu: [Ad Soyad]
 E-Posta: varlik.sedat@gmail.com
 Telefon: 0224 513 1728

Gemlik Anadolu İmam Hatip Lisesi Yönetimi
 Tarih: 01.01.2025

Bu kılavuz, **çocukların interneti güvenli, bilinçli ve sorumlu bir şekilde kullanmalarını sağlamak** amacıyla hazırlanmıştır. Tüm velilerimizin **çocuklarıyla birlikte bu kuralları gözden geçirmeleri ve dijital güvenlik konusunda bilinçli olmaları** önemlidir.

 Dijital dünya güvenli bir yer olabilir, yeter ki bilinçli kullanım ile koruma sağlansın!

SİBER GÜVENLİK VE KİŞİSEL VERİLERİN KORUNMASI POLİTİKASI

 Yayın Tarihi: 01.01.2025
 Belge No: [Belge Numarası]
 Hazırlayan: Gemlik Anadolu İmam Hatip Lisesi Yönetimi

---

1. Giriş

Bu politika, **öğrencilerin, velilerin, öğretmenlerin ve okul personelinin dijital ortamda güvenliğini sağlamak ve kişisel verilerin korunmasını garanti altına almak amacıyla** oluşturulmuştur.

✅**Siber güvenlik**, öğrencilerin, velilerin ve okul çalışanlarının **bilgi sistemlerini kötü amaçlı yazılımlardan, yetkisiz erişimden ve veri ihlallerinden korumayı amaçlar**.
✅**Kişisel verilerin korunması**, öğrencilerin, velilerin ve çalışanların kimlik bilgileri, sağlık kayıtları, akademik verileri gibi **özel bilgilerin izinsiz paylaşılmasını veya kötüye kullanılmasını önlemeyi hedefler**.

---

2. Siber Güvenlik Politikası

Okul yönetimi, öğretmenler, öğrenciler ve veliler, **siber güvenlik kurallarına uymakla yükümlüdür**.

2.1. Alınacak Siber Güvenlik Önlemleri

 Güçlü şifre politikası uygulanacaktır.
 Yetkisiz erişimi önlemek için çok faktörlü kimlik doğrulama (MFA) kullanılacaktır.
 Öğrenci ve personel cihazlarına güncel antivirüs yazılımları yüklenecektir.
 Tüm okul ağı güvenlik duvarları ile korunacaktır.
 Kapsamlı veri yedekleme politikası uygulanacaktır.
 USB ve harici belleklerin izinsiz kullanımı sınırlandırılacaktır.

2.2. Okul Ağı ve Cihaz Kullanım Kuralları

 Okul Wi-Fi ağı sadece eğitim amaçlı kullanılmalıdır.
 Yetkisiz cihazların okul ağına bağlanması yasaktır.
 Okul bilgisayarlarında yalnızca onaylı yazılımlar kullanılmalıdır.
 Sosyal medya, oyun ve eğlence sitelerine giriş okul tarafından belirlenen sınırlar içinde tutulmalıdır.

2.3. Siber Tehditlere Karşı Korunma

 Phishing (oltalama) saldırılarına karşı dikkatli olunmalı, şüpheli e-postalar açılmamalıdır.
 Dijital dolandırıcılık ve sahte kimliklere karşı bilinçli olunmalıdır.
 İzinsiz veri erişimi ve veri sızıntıları konusunda farkındalık oluşturulmalıdır.
 Siber saldırı durumunda IT birimine veya okul yönetimine hemen haber verilmelidir.

---

3. Kişisel Verilerin Korunması Politikası

Kişisel verilerin korunması, **6698 sayılı Kişisel Verilerin Korunması Kanunu (KVKK)** ve ilgili mevzuata uygun şekilde sağlanmalıdır.

3.1. Kişisel Veri Nedir?

 Öğrenci bilgileri (Ad, Soyad, TC Kimlik Numarası, Adres, Doğum Tarihi)
 Akademik kayıtlar (Notlar, Devam Durumu, Sınav Sonuçları)
 Sağlık bilgileri (Acil Durum Kayıtları, Sağlık Raporları)
 Veli ve öğretmen bilgileri (İletişim Bilgileri, Kimlik Bilgileri)

3.2. Kişisel Verilerin İşlenme Prensipleri

 Veri toplama, yalnızca gerekli durumlarda ve açık rıza alınarak yapılacaktır.
 Veriler, üçüncü şahıslarla veya yetkisiz kişilerle paylaşılmayacaktır.
 Öğrenci ve velilerin rızası olmadan, fotoğraf ve kişisel bilgiler sosyal medyada paylaşılmayacaktır.
 Öğrencilerin akademik kayıtları ve özel bilgileri yalnızca yetkili okul personeli tarafından erişilebilir olacaktır.

3.3. Kişisel Verilere Yetkisiz Erişim Nasıl Önlenir?

 Öğrenci ve öğretmen hesapları için güçlü şifreler oluşturulmalıdır.
 Okul yönetimi, kişisel verileri şifreli ve güvenli veri tabanlarında saklamalıdır.
 Yetkisiz erişimi önlemek için personel ve öğrencilerin hesapları düzenli olarak kontrol edilmelidir.
 Okul, kişisel veri ihlalleri hakkında çalışanları ve öğrencileri bilgilendirecek eğitimler düzenlemelidir.

---

4. Velilerin Bilmesi Gerekenler

 Çocukların kişisel bilgilerini (adres, okul adı, doğum tarihi) sosyal medyada paylaşmamalarını sağlayın.
 Öğrencinizin çevrim içi platformlarda yalnızca güvenli ve resmi okul sistemlerini kullanmasını teşvik edin.
 Şüpheli e-postalara, bilinmeyen bağlantılara ve sahte sitelere karşı dikkatli olun.
 Çocuğunuzun dijital güvenliği hakkında okul yönetimiyle iş birliği içinde olun.

---

5. Siber Güvenlik ve Kişisel Veri İhlallerinde Ne Yapılmalı?

 Eğer bir güvenlik açığı veya kişisel veri ihlali fark edilirse:
 Okul yönetimine veya bilgi güvenliği sorumlusuna hemen bildirin.
 İlgili veri sızıntısını belgeleyin ve IT departmanına iletin.
 Yetkililer gerekli teknik ve hukuki önlemleri alacaktır.

---

6. Okul Yönetimi ve Yetkili Kişiler

 Bilgi Güvenliği ve KVKK Sorumlusu: [Ad Soyad]
 E-Posta: varlik.sedat@gmail.com
 Telefon: 0224 513 1728

Gemlik Anadolu İmam Hatip Lisesi Yönetimi
 Tarih: 01.01.2025

Dijital dünyada güvenlik, sadece teknik önlemlerle değil, bilinçli kullanım ile sağlanır!

SİBER ZORBALIK VE GÜVENLİ İNTERNET KULLANIMI POLİTİKASI

 Yayın Tarihi: 01.01.2025
 Belge No: [Belge Numarası]
 Hazırlayan: Gemlik Anadolu İmam Hatip Lisesi Yönetimi

---

1. Giriş

Bu politika, öğrencilerin **siber zorbalıktan korunması**, **güvenli internet kullanımının teşvik edilmesi** ve **dijital ortamda etik davranışların benimsenmesi** amacıyla oluşturulmuştur.

 Siber zorbalık, bir bireyin veya grubun, dijital platformlar aracılığıyla kasıtlı olarak başkalarını rahatsız etmesi, tehdit etmesi, aşağılaması veya manipüle etmesidir.
 Güvenli internet kullanımı, öğrencilerin çevrim içi tehditlerden korunarak **bilinçli ve sorumlu bir şekilde interneti kullanmalarını** sağlamaktır.

---

2. Siber Zorbalık Nedir?

Siber zorbalık, bireylerin **dijital ortamda psikolojik veya duygusal zarar görmesine neden olabilecek her türlü kötü niyetli davranışı** içerir.

2.1. Siber Zorbalık Türleri

❌**Hakaret ve Küfür:** Çevrim içi ortamda kişilere hakaret etmek veya kötü sözler yazmak.
❌**Tehdit ve Şantaj:** Bireyleri korkutmak veya zarar vermekle tehdit etmek.
❌**Dedikodu ve Yalan Haber Yayma:** Bir kişi hakkında asılsız bilgiler paylaşmak.
❌**İfşa ve Gizliliği İhlal:** Özel bilgileri, fotoğrafları veya mesajları izinsiz paylaşmak.
❌**Sahte Hesap Açma:** Bir başkasının kimliğine bürünerek zarar verici içerikler paylaşmak.
❌**Sosyal Dışlama:** Kişileri grup sohbetlerinden veya çevrim içi etkinliklerden dışlamak.

---

3. Siber Zorbalıkla Mücadele İçin Alınacak Önlemler

 Öğrenciler, veliler ve öğretmenler için farkındalık eğitimleri düzenlenmelidir.
 Siber zorbalığa uğrayan öğrenciler desteklenmeli ve okul rehberlik servisine yönlendirilmelidir.
 Okul yönetimi, çevrim içi zorbalık vakalarını takip etmeli ve gerekli yaptırımları

uygulamalıdır.
□ Öğrencilerin güvenli platformları kullanmaları teşvik edilmelidir.
□ Siber zorbalıkla ilgili şikayet mekanizmaları oluşturulmalıdır.

3.1. Siber Zorbalıkla Karşılaşan Öğrencilerin Yapması Gerekenler

✅Zorbalık içeren mesajları veya içerikleri cevaplamayın.
✅Zorbalıkla ilgili ekran görüntüsü alın ve kanıtları saklayın.
✅Durumu okul rehberlik servisine, öğretmene veya bir yetişkine bildirin.
✅Şüpheli kişileri veya hesapları sosyal medya platformlarında engelleyin.

---

4. Güvenli İnternet Kullanımı İçin Kurallar

4.1. Genel Güvenlik Önlemleri

□ Kişisel bilgilerinizi (adres, telefon, okul adı) yabancılarla paylaşmayın.
□ Güçlü şifreler oluşturun ve kimseyle paylaşmayın.
□ Şüpheli bağlantılara ve bilinmeyen e-postalara tıklamayın.
□ Çevrim içi arkadaşlıklar kurarken dikkatli olun, gerçek kimliğinden emin olmadığınız kişilere güvenmeyin.
□ Siber zorbalık, dolandırıcılık veya zararlı içeriklerle karşılaştığınızda yetişkinlere bildirin.

4.2. Sosyal Medya Kullanım Kuralları

□ Paylaşımlarınızı herkese açık yapmayın, gizlilik ayarlarınızı kontrol edin.
□ Tanımadığınız kişilerden gelen arkadaşlık isteklerini kabul etmeyin.
□ Başkalarının izni olmadan fotoğraf veya video paylaşmayın.
□ Siber zorbalığa karşı duyarlı olun ve zarar verici içeriklere ortak olmayın.
□ Başkalarına saygılı davranın, empati kurun ve etik kurallara uyun.

4.3. Ebeveynler İçin Güvenli İnternet Önerileri

□□□ Çocuklarınızın hangi siteleri ziyaret ettiğini ve kiminle iletişim kurduğunu takip edin.
□□□ Aile koruma programları ve filtreleme sistemleri kullanın.
□□□ Çocuğunuzla siber zorbalık ve internetin güvenli kullanımı hakkında konuşun.
□□□ Onları çevrim içi ortamda destekleyin ve karşılaştıkları sorunları paylaşmaları için teşvik edin.

---

5. Siber Güvenlik ve Zorbalıkla Mücadelede Okulun Rolü

 Okul yönetimi, öğrencilerin dijital güvenliğini sağlamakla yükümlüdür.
 Öğrencilere yönelik düzenli siber güvenlik ve etik internet kullanımı eğitimleri verilmelidir.
 Okul içi internet kullanımı denetlenmeli, güvenli eğitim platformları sağlanmalıdır.
 Siber zorbalıkla ilgili öğrencilerin şikayetlerini iletebileceği güvenli bir sistem oluşturulmalıdır.

---

6. Siber Zorbalık ve Güvenli İnternet Kullanımı İhlallerinde Uygulanacak Yaptırımlar

 Siber zorbalık yapan öğrenciler için aşağıdaki disiplin önlemleri uygulanabilir:
 Rehberlik servisi ile görüşme ve bilinçlendirme eğitimi.
 Velilere bilgilendirme yapılması.
 Okul disiplin kurulu tarafından yaptırım uygulanması.
 Gerekli durumlarda yasal mercilere başvuru yapılması.

---

7. Acil Durumda Yapılması Gerekenler

 Eğer bir öğrenci siber zorbalığa uğrarsa:
 Okul rehberlik servisine veya bir öğretmene durumu bildirin.
 Ekran görüntüleri alarak kanıtları saklayın.
 Sosyal medya platformlarında şikayet mekanizmalarını kullanın.
 Gerekirse yasal mercilere başvurun (BTK, Siber Suçlarla Mücadele Birimi vb.).

---

8. İletişim Bilgileri

 Bilgi Güvenliği ve Rehberlik Sorumlusu: [Ad Soyad]
 E-Posta: varlik.sedat@gmail.com
 Telefon: 0224 513 1728

 Dijital dünyada güvenlik, bilinçli kullanım ve karşılıklı saygı ile sağlanır!

OKUL TEKNOLOJİ VE BİLİŞİM GÜVENLİĞİ PROSEDÜRLERİ

 Yayın Tarihi: 01.01.2025
 Belge No: [Belge Numarası]
 Hazırlayan: Gemlik Anadolu İmam Hatip Lisesi Bilgi Teknolojileri ve Güvenlik Birimi

---

1. Amaç

Bu prosedür, **öğrencilerin, öğretmenlerin ve okul çalışanlarının bilişim sistemlerini güvenli ve verimli bir şekilde kullanmalarını sağlamak** ve **dijital güvenliği artırmak** amacıyla hazırlanmıştır.

 Hedefler:
✔ Okul sistemlerinin yetkisiz erişimden korunması
✔ Öğrenci ve öğretmen bilgilerinin gizliliğinin sağlanması
✔ Çevrim içi tehditlere karşı okul ağının korunması
✔ Eğitim sürecinde teknoloji kullanımının güvenli hale getirilmesi

---

2. Genel Teknoloji ve Bilişim Güvenliği İlkeleri

 Okulun tüm bilişim sistemleri yalnızca eğitim ve yönetim amaçlı kullanılmaktadır.
 Tüm kullanıcılar (öğrenciler, öğretmenler, idari personel) güçlü şifreler kullanmaktadır.
 Yetkisiz kişilerin okul bilişim sistemlerine erişimi engellenmektedir.
 Tüm yazılımlar ve sistemler düzenli olarak güncellenmektedir.
 Okulda kullanılan cihazlar, kötü amaçlı yazılımlara karşı korunmalıdır.
 Öğrencilerin kişisel ve akademik bilgileri, okul politikalarına uygun olarak korunmalıdır.

---

3. Okulda Kullanılan Bilişim Sistemleri

 Okul Sunucuları ve Ağ Altyapısı:
 Okul içi sunuculara ve ağ altyapısına yalnızca yetkili personel erişebilir.
 Ağ bağlantıları, güvenlik duvarları ve antivirüs yazılımları ile korunmalıdır.
 Kablosuz ağlar (Wi-Fi) farklı gruplara ayrılmalı: **Öğrenci Ağı, Öğretmen Ağı, Misafir Ağı**.
 Yetkisiz cihazların okul ağına bağlanması engellenmelidir.

 Okul Bilgisayarları ve Cihazları:
 Bilgisayarlar, tabletler ve akıllı tahtalar yalnızca eğitim amaçlı kullanılmalıdır.
 İzinsiz yazılım yüklenmesi yasaktır.
 Bilgisayar laboratuvarlarında USB kullanımı sınırlandırılmalıdır.
 Tüm cihazlar düzenli olarak virüs taramasından geçirilmelidir.

 İnternet ve Sosyal Medya Kullanımı:
 Okulda kullanılan internet filtrelenmeli ve tehlikeli içeriklere erişim engellenmelidir.
 Sosyal medya platformlarına erişim yalnızca eğitim amaçlı belirlenen saatlerde sağlanmalıdır.
 Öğrenciler ve personel, okul ile ilgili özel bilgileri sosyal medyada paylaşmamalıdır.

 E-Posta ve Dijital Haberleşme:
 Resmi yazışmalar için sadece okulun sağladığı e-posta adresleri kullanılmalıdır.
 Şüpheli e-postalar açılmamalı ve bilinmeyen bağlantılara tıklanmamalıdır.
 Hassas bilgiler içeren e-postalar şifrelenerek gönderilmelidir.

---

4. Kullanıcı Yetkilendirme ve Erişim Kontrolleri

Öğrenciler ve öğretmenler, okul sistemlerine yalnızca kendilerine verilen kullanıcı adı ve şifre ile erişebilir.
Kullanıcı yetkileri, görev ve sorumluluklara göre belirlenmelidir.
Güçlü şifre politikası uygulanmalı (en az 8 karakter, harf, rakam ve özel karakter içermelidir).
Yetkisiz kişilerin okul sunucularına veya öğrenci kayıt sistemine erişimi engellenmelidir.
Düzenli olarak erişim kayıtları incelenmeli ve yetkisiz girişler raporlanmalıdır.

---

5. Bilgi Güvenliği ve Kişisel Verilerin Korunması

Öğrenci, öğretmen ve veli bilgileri gizli tutulmalıdır.
Veriler yalnızca yetkili kişiler tarafından erişilebilir olmalıdır.
Kişisel veriler şifreli sunucularda saklanmalıdır.
Ders notları, sağlık bilgileri, kimlik bilgileri gibi veriler yetkisiz kişilerle paylaşılmamalıdır.
Okul tarafından paylaşılan dijital içerikler, KVKK (Kişisel Verilerin Korunması Kanunu) ile uyumlu olmalıdır.

---

6. Siber Güvenlik ve Veri Koruma Önlemleri

Tüm okul sistemleri ve cihazlar, düzenli olarak antivirüs yazılımı ile taranmalıdır.
Güncellenmeyen veya güvenlik açığı bulunan yazılımlar kullanılmamalıdır.
Tüm kritik veriler yedeklenmeli ve yedekler güvenli bir yerde saklanmalıdır.

 Okul, siber saldırılara karşı firewall (güvenlik duvarı) ve IDS/IPS (saldırı tespit ve engelleme sistemleri) kullanmalıdır.
 Öğrencilere ve öğretmenlere dijital güvenlik eğitimi verilmelidir.

---

7. Veri Yedekleme ve Kurtarma Prosedürleri

 Veri yedekleme haftalık olarak yapılmalı ve güvenli bir ortamda saklanmalıdır.
 Yedekleme işlemi, bulut sistemleri veya harici sunucular aracılığıyla gerçekleştirilmelidir.
 Olası bir veri kaybı durumunda acil müdahale prosedürleri uygulanmalıdır.
 Felaket durumlarında (siber saldırı, doğal afet vb.) veri kurtarma planları oluşturulmalıdır.

---

8. Okulda Siber Güvenlik İhlallerinde Uygulanacak Yaptırımlar

 Aşağıdaki ihlaller tespit edildiğinde okul yönetimi tarafından yaptırımlar uygulanır:
 Yetkisiz erişim girişimleri ve hackleme teşebbüsleri.
 Kötü amaçlı yazılım veya zararlı içerik kullanımı.
 Okul sistemlerine izinsiz giriş yapma veya veri sızdırma.
 Siber zorbalık ve çevrim içi taciz vakaları.
 Güvenlik açıklarını kötüye kullanma veya okulun itibarını zedeleyici paylaşımlar yapma.

 İhlallerin tekrarlanması durumunda disiplin prosedürleri uygulanır ve gerekirse yasal mercilere başvuru yapılır.

---

9. Bilgi Güvenliği İhlal Bildirimi

 Siber güvenlik ihlali veya veri sızıntısı fark eden kişiler derhal okul yönetimine haber vermelidir.
 İhlalin kaynağı ve etkileri araştırılmalı, gerekli önlemler alınmalıdır.
 Olası güvenlik tehditleri okul bilişim birimi tarafından raporlanmalıdır.

 İhlal bildirimleri için:
 E-Posta: varlik.sedat@gmail.com
 Telefon: 0224 513 1728

 Teknoloji güvenliği herkesin sorumluluğudur! Güvenli ve bilinçli bir dijital ortam için kurallara uyalım.

Farkındalık ve Eğitim Materyalleri

Okulda **teknoloji, siber güvenlik ve güvenli internet kullanımı** konularında farkındalık yaratmak ve öğrencileri bilinçlendirmek için çeşitli eğitim materyalleri hazırlanmalıdır.

---

1. Temel Eğitim Materyalleri

 Afişler ve Posterler:

- **Güçlü Şifre Kullanımı**
- **Güvenli Sosyal Medya Kullanımı**
- **Siber Zorbalık Nedir ve Nasıl Önlenir?**
- **Dijital Ayak İzi ve Gizliliğin Önemi**
- **Phishing (Oltalama) Saldırılarına Karşı Önlemler**

 El Kitapları ve Kılavuzlar:

- **Öğrenciler İçin Siber Güvenlik Rehberi**
- **Veliler İçin Güvenli İnternet Kullanımı Kılavuzu**
- **Öğretmenler İçin Dijital Güvenlik Eğitimi Rehberi**

 Eğitim Videoları ve Animasyonlar:

- **"Siber Zorbalığa Karşı Ne Yapmalıyım?"**
- **"Güçlü Bir Şifre Nasıl Oluşturulur?"**
- **"Güvenli Sosyal Medya Kullanımı"**
- **"Kişisel Verilerimizi Nasıl Koruyabiliriz?"**

 Sunumlar ve Slaytlar:

- **Siber Güvenlik Temelleri**
- **Veri Gizliliği ve KVKK (Kişisel Verilerin Korunması Kanunu)**
- **Çevrim içi Tehditler ve Korunma Yöntemleri**

---

2. Uygulamalı Eğitimler ve Atölyeler

 Simülasyonlar ve Tatbikatlar:

- **Oltalama (Phishing) E-postası Testi:** Öğrencilere sahte e-posta örnekleri gösterilerek oltalama saldırılarını tanımaları sağlanır.
- **Siber Zorbalık Senaryoları:** Gerçek olaylardan örnekler verilerek farkındalık oluşturulur.

 Dijital Güvenlik Çalıştayları:

- **Güvenli Şifre Oluşturma Atölyesi**
- **Dijital Medya Okuryazarlığı Eğitimi**
- **Veri Güvenliği ve Şifreleme Uygulamaları**

Okul Tabanlı Bilgilendirme Günleri:

- **Siber Güvenlik Haftası Etkinlikleri**
- **Ebeveynler İçin Teknoloji ve Güvenlik Seminerleri**

---

3. İnteraktif Eğitim Araçları

Online Testler ve Anketler:

- **Siber Güvenlik Bilgi Testi**
- **Güvenli İnternet Kullanımı Anketi**

Eğitsel Oyunlar:

- **Siber Güvenlik Kahoot! veya Quizizz Testleri**
- **Dijital Güvenlik Macera Oyunu (Örneğin: "Kimlik Avından Kurtul!")**

Güvenli İnternet Kullanımı İçin Mobil Uygulamalar:

- **Google "Be Internet Awesome" gibi interaktif öğrenme araçları**
- **Cyberwise veya Digital Compass gibi dijital okuryazarlık uygulamaları**

---

4. Okul Politikaları ve Bilgilendirme Materyalleri

Öğrencilere, öğretmenlere ve velilere dağıtılacak broşürler ve bilgilendirme kitapçıkları hazırlanmalıdır.
Dijital Güvenlik Politikası okul web sitesinde paylaşılmalıdır.
Sınıflara güvenli internet kullanımını anlatan bilgi panoları yerleştirilmelidir.
Velilere ve öğrencilere düzenli bilgilendirme e-postaları gönderilmelidir.

Teknoloji güvenli bir şekilde kullanıldığında öğrenmeyi destekler! Farkındalık yaratmak için bu materyalleri etkili bir şekilde kullanabiliriz.