BAĞCILAR BİLİM VE SANAT MERKEZİ

E-GÜVENLİK POLİTİKASI ve KURALLARI

1. Amaç

Bağcılar Bilim ve Sanat Merkezi, dijital ortamların güvenli ve etkili bir şekilde kullanılmasını sağlamak, öğrencilerimizin, öğretmenlerimizin ve diğer paydaşlarımızın çevrimiçi risklerden korunmasını güvence altına almak amacıyla e-güvenlik politikası geliştirmiştir. Bu politika, bilgi iletişim teknolojilerinin (BİT) faydalarından maksimum düzeyde yararlanmayı desteklerken, olası riskleri en aza indirmeyi hedefler.

2. Temel Prensipler

- Merkezimiz, MEB'in sağladığı güvenli internet filtreleme altyapısını kullanarak zararlı içeriklere erişimi engeller.
- Tüm dijital cihazlarda ve sistemlerde güncel antivirüs ve güvenlik yazılımları bulunur.
- Çevrimiçi ortamlarda etik kurallar ve dijital davranışlar konularında tüm paydaşlara rehberlik edilir.
- Kişisel verilerin korunması için 6698 sayılı Kişisel Verilerin Korunması Kanunu'na tam uyum sağlanır.
- Öğrenciler, veliler ve çalışanlar arasında dijital vatandaşlık bilincini geliştirmek için seminerler ve eğitim programları düzenlenir.

3. Kapsam

Bu politika;

- Merkezimize ait bilgisayar sistemlerini, tabletleri, akıllı tahtaları, sunucuları ve ağları kullanan tüm öğrenciler, öğretmenler, veliler, ziyaretçiler ve diğer paydaşları kapsar.
- Okul içi ve dışı erişimlerde kullanılan cihazları ve çevrimiçi kaynakları içerir.

4. E-Güvenlik Politikası İlkeleri

4.1. Güvenli İnternet Erişimi ve Cihaz Kullanımı

- İnternet erişimi yalnızca eğitim ve araştırma amacıyla kullanılmak üzere güvenli bir ağ üzerinden sağlanır.
- Öğrenciler, ders saatleri içinde mobil cihazlarını ve kişisel teknolojik cihazlarını kullanamazlar. Özel durumlar, öğretmenin iznine tabidir.
- Çocukların teknoloji bağımlılığı ve siber zorbalık gibi konularda bilinçlenmesi için rehberlik servisi düzenli eğitimler düzenler.

4.2. Çevrimiçi İçerik Yönetimi

- Merkezimizin internet sitesi ve sosyal medya hesaplarında paylaşılan tüm içerikler idare onayından geçer ve gizlilik kurallarına uygun olarak paylaşılır.
- Öğrencilerin yüzleri, velilerin açık onayı olmaksızın sosyal medya platformlarında veya çevrimiçi ortamlarda paylaşılmaz.
- Çevrimiçi ders materyalleri ve kaynaklar, güvenilir platformlardan temin edilir ve telif haklarına uygun olarak kullanılır.

4.3. Kişisel Verilerin Korunması

- Öğrenci ve velilere ait iletişim bilgileri, sadece ilgili idari personelin erişimine açıktır ve üçüncü kişilerle paylaşılmaz.
- Tüm personel ve öğrenciler, dijital ortamlarda kişisel bilgilerin korunmasına yönelik bilinçlendirilir.

4.4. Eğitim ve Farkındalık Çalışmaları

Öğrenciler İçin:

- **Güvenli İnternet Kullanımı Eğitimleri:** Öğrencilere internet etiği, bilgi güvenliği, güvenli veri paylaşımı, siber zorbalıkla başa çıkma yöntemleri ve dijital bağımlılıkla mücadele gibi konularda düzenli eğitimler verilir. Bu eğitimler, yaş gruplarına uygun içeriklerle planlanır ve etkin katılım teşvik edilir.
- **Dijital Vatandaşlık Eğitimi:** Öğrencilere çevrimiçi ortamlarda etik davranışlar, dijital izlerinin farkında olma, online kaynakları doğru ve etkili kullanma, bilgi doğrulama teknikleri gibi temel dijital vatandaşlık becerileri kazandırılır.
- **Uygulamalı Çalışmalar:** Bilgi güvenliği farkındalığını artırmak için "Güvenli Parola Oluşturma" atölyeleri, "Siber Zorbalık Senaryoları" ile uygulamalı problem çözme etkinlikleri düzenlenir.
- **Ödüllü Yarışmalar ve Etkinlikler:** Güvenli internet kullanımı ile ilgili afiş, kısa film ve hikâye yarışmaları düzenlenerek öğrencilerin yaratıcı yöntemlerle konuya katılımı sağlanır.

Veliler İçin:

- **Dijital Rehberlik Seminerleri:** Velilere yönelik düzenli olarak "Çocuklar ve Dijital Dünya", "Sosyal Medya Kullanımında Ebeveynlerin Rolü" ve "Siber Zorbalık ve Ebeveyn Farkındalığı" gibi konularda seminerler gerçekleştirilir.
- **Bilgilendirme Bültenleri:** Velilere, güvenli internet kullanımı ve çevrimiçi tehditlere karşı alınabilecek önlemleri içeren bilgilendirme dokümanları ve rehberler sunulur.
- **Destek Hattı ve Kaynak Paylaşımı:** Veliler için çevrimiçi güvenlik sorunlarında destek alabilecekleri kaynakların ve iletişim bilgilerin yer aldığı bir rehber hazırlanır.

Öğretmen ve Personel İçin:

- **Mesleki Gelişim Eğitimleri:** Öğretmenler ve merkez personeli, siber güvenlik, dijital veri koruma, çevrimiçi içerik yönetimi ve dijital vatandaşlık konularında düzenli olarak Milli Eğitim Bakanlığı'nın sağladığı eğitim programlarına katılır.

- **Kurum İçi Eğitim Programları:** Merkez bünyesinde öğretmenler tarafından "Güvenli Dijital Sınıf Yönetimi" ve "Çevrimiçi Eğitim Platformlarının Etkin Kullanımı" gibi konularda bilgi ve deneyim paylaşımına yönelik kurum içi eğitimler düzenlenir.
- **Rol Model Davranışlar:** Öğretmenlerin güvenli internet kullanımı, etik çevrimiçi davranışlar ve bilgi paylaşımı konularında öğrencilere örnek olmaları teşvik edilir.

Genel Bilinçlendirme Çalışmaları:

- **Güvenli İnternet Günü Etkinlikleri:** Her yıl Şubat ayında düzenlenen Güvenli İnternet Günü kapsamında, konferanslar, atölyeler ve farkındalık kampanyaları gerçekleştirilir.
- **Sabit Bilgilendirme Panoları:** Merkezde, dijital güvenlik ve çevrimiçi davranışlarla ilgili bilgilendirici afişler ve duyuruların yer aldığı sabit panolar bulundurulur.
- **Online Platformlarda Bilinçlendirme:** Merkezimizin resmi internet sitesi ve sosyal medya hesaplarında e-güvenlik konusunda bilgilendirici içerikler paylaşılır. Eğitim videoları, rehber dokümanlar ve kısa bilgilendirme mesajları yayımlanır.

Özel Gruplar İçin:

- **Yetenekli Öğrencilerle Derinleşen Eğitimler:** Teknolojiye özel ilgisi olan öğrenciler için siber güvenlik, programlama konularında ileri seviye eğitimler düzenlenir.
- **Farklı Düzeylerde Bilinçlendirme:** Özel eğitim gereksinimi olan öğrenciler için daha sade ve görsel ağırlıklı bilinçlendirme programları hazırlanır.

4.5. Kabul Edilebilir Kullanım Politikası (AUP)

- Merkezdeki cihaz ve ağlar yalnızca eğitimle ilgili faaliyetler için kullanılabilir.
- Kullanıcılar, okul sistemlerine ait hesaplarını koruma sorumluluğuna sahiptir. Şifreler paylaşılmamalı ve düzenli olarak güncellenmelidir.
- Zararlı yazılım, uygunsuz içerik ve korsan yazılım kullanımı kesinlikle yasaktır.

4.6. Çevrimiçi İhlallere Müdahale

- Çevrimiçi bir ihlal durumunda, ilgili durum yönetime bildirilir ve gerekli önlemler alınır.
- İhlal ciddi bir disiplin cezası gerektiriyorsa, durum yasal mercilere iletilebilir.

5. Sorumluluklar

5.1. Yönetim Ekibi

- Politikanın hazırlanması, uygulanması ve gözden geçirilmesinden sorumludur.
- Eğitim içeriklerini ve çevrimiçi güvenlik prosedürlerini düzenli olarak günceller.

5.2. Öğretmenler

- Çevrimiçi güvenlik konusunda öğrenciler için rol model olur.

- Ders müfredatlarına, eğitim materyallerine ve ders içeriklerine e-güvenlik prensiplerini entegre eder.

5.3. Öğrenciler

- Çevrim içi ortamda etik davranışlar sergiler ve karşılaştıkları sorunları öğretmenleriyle paylaşır.
- Güvenli şifreleme, güvenli veri paylaşımı gibi temel güvenlik kurallarına uyar.

5.4. Veliler

- Çocuklarının internet kullanımını takip eder ve güvenli davranışları teşvik eder.
- Okulun e-güvenlik politikalarına uyum sağlanmasını destekler.

6. Gözden Geçirme ve Güncelleme

Bu politika, her yıl Bilgi Teknolojileri Birimi tarafından her yıl Ocak ayında gözden geçirilir ve güncellenir. Politika değişiklikleri yönetim onayına sunularak yürürlüğe girer.

7. Sonuç

Bağcılar Bilim ve Sanat Merkezi, öğrencilerinin ve çalışanlarının dijital ortamlarda güvenliğini sağlamak için sürekli iyileştirme anlayışıyla hareket eder. Bu politika, tüm paydaşların katkısıyla etkili bir şekilde uygulanarak sürdürülecektir.

Bağcılar Bilim ve Sanat Merkezi Yönetimi