



ŞAHİNLER ORTAOKULU

eSafety Label

OKUL GÜVENLİK PLANI

1. GİRİŞ

21. yüzyılın bilgi toplumuna dönüşüm süreciyle birlikte teknoloji, yaşamın tüm alanlarında olduğu gibi eğitimde de merkezi bir konuma yerleşmiştir. Bilgiye erişimi kolaylaştıran, öğrenme süreçlerini hızlandıran ve bireyler arası etkileşimi artıran dijital araçlar, öğrencilerin hem akademik hem sosyal gelişimini destekleyici niteliktedir. Bu nedenle teknolojiyi bilinçli, güvenli ve etik bir biçimde kullanmak günümüz eğitim kurumlarının öncelikli sorumluluklarından biri hâline gelmiştir.

Özellikle uluslararası çevrim içi iş birliğini esas alan eTwinning projeleri, öğrencilerin dijital okuryazarlık, medya farkındalığı ve kültürlerarası iletişim becerilerini güçlendirirken, aynı zamanda onları bazı dijital tehditlerle de karşı karşıya bırakabilmektedir. Bu tehditler arasında kişisel verilerin izinsiz paylaşımı, siber zorbalık, zararlı içeriklere maruz kalma ve dijital bağımlılık gibi riskler yer almaktadır.

Şahinler Ortaokulu olarak yürüttüğümüz eTwinning projelerinde, öğrencilerimizin bu dijital risklerden korunmalarını sağlamak, güvenli dijital ortamlar oluşturmak ve tüm paydaşların sorumluluklarını netleştirmek amacıyla bu eGüvenlik Okul Güvenlik Planı hazırlanmıştır.

2. AMAÇLAR

- Dijital güvenlik bilincini tüm okul topluluğunda artırmak
- Öğrencilerin interneti güvenli, etik ve verimli biçimde kullanmalarını sağlamak
- eTwinning projelerinde dijital haklar ve sorumluluklar konusunda rehberlik sunmak
- Okulun bilişim altyapısını siber tehditlere karşı korumak
- Velileri evdeki dijital ortam güvenliği konusunda bilgilendirmek
- Siber olaylara karşı hızlı ve etkili müdahale mekanizmaları oluşturmak

3. HEDEF GRUPLAR

- Öğrenciler
- Öğretmenler
- Okul Yöneticileri
- Veliler
- Proje Ortakları

4. RİSK ANALİZİ

Risk Alanı	Olası Tehlikeler
Sosyal Medya Kullanımı	Kimlik hırsızlığı, özel hayatın gizliliğinin ihlali, siber zorbalık
eTwinning/TwinSpace Platformları	Telif hakkı ihlali, veri sızıntısı, izinsiz içerik paylaşımı
Okul Wi-Fi ve Bilgisayar Ağı	Zararlı yazılım bulaşması, filtrelenmemiş içeriklere erişim
Cihaz Kullanımı	Kötü amaçlı yazılımlar, veri kaybı, izinsiz dosya aktarımı
E-posta ve Mesajlaşma	Ölçüleme saldırıları (phishing), spam içerikler
Ev Ortamı ve Veli Denetimi	Aşırı ekran süresi, içerik kontrolsüzlüğü, çevrim içi yabancı kişilerle temas

5. GÜVENLİK STRATEJİLERİ VE UYGULAMA ADIMLARI

5.1. Teknik Güvenlik Önlemleri

- İnternet filtreleme sistemleri aktif hâle getirilir (BTK Güvenli Çocuk Profili vb.).
- Tüm okul cihazlarında lisanslı, güncel antivirüs yazılımları kurulu olmalıdır.
- Ortak cihazlarda kullanıcı giriş sistemleri uygulanır; yetkisiz erişim engellenir.
- USB ve harici cihazlar sadece öğretmen onayıyla kullanılabilir.
- TwinSpace, e-posta ve diğer platformlardaki oturumlar kapatılmadan bırakılmamalıdır.
- Proje dosyaları haftalık olarak okul sunucularına veya güvenli bulut sistemlerine yedeklenir.

5.2. Pedagojik Güvenlik Önlemleri

- Öğrencilere yönelik yılda en az 2 kez "Dijital Güvenlik ve Etik Kullanım" temalı seminer düzenlenir.
- Bilişim Teknolojileri ve Rehberlik derslerinde siber zorbalık, dijital haklar, güvenli sosyal medya kullanımı konularına müfredat düzeyinde yer verilir.
- eTwinning projeleri kapsamında içerik üretimi yapan öğrencilere telif hakkı ve kaynak gösterme eğitimi verilir.
- Öğrencilerle birlikte “Dijital Davranış Kuralları (Netiket)” listesi oluşturulur ve sınıflara asılır.

5.3. İdari Güvenlik Önlemleri

- Öğrenci ve velilere dijital güvenlik politikası yazılı olarak bildirilir.
- Velilerden kişisel veri işleme (görsel, ses, ad-soyad) izin belgeleri alınır.
- Güvenlik ihlallerinde başvurulacak müdahale ve raporlama prosedürleri belirlenir.
- Okul içi güvenlik denetimleri bilişim teknolojileri sorumlusu tarafından her dönem başında yapılır.

6. OLAY MÜDAHALE PROTOKOLÜ

Aşama	Açıklama
1. Olay Bildirimi	Öğrenci veya öğretmen ilgili durumu okul idaresine iletir.
2. Ön İnceleme	Okul idaresi ve rehber öğretmen olayı gizlilik esasına göre değerlendirir.
3. Müdahale	Gerekirse teknik önlem (şifre sıfırlama, cihaz izolasyonu) alınır.
4. Veli Bilgilendirme	Olayın niteliğine göre velilere bilgi verilir.
5. Kayıt ve Raporlama	Tüm olay e-Güvenlik Olay Formu ile belgelenir.
6. İyileştirme Adımı	Olaydan elde edilen bulgularla politika geliştirmeleri yapılır.

7. VELİ KATILIMI VE EVDE GÜVENLİK

- Velilere yönelik "Evde Dijital Güvenlik ve Ebeveyn Denetimi" eğitimi organize edilir.
- Ailelere filtreleme yazılımı ve ekran süresi denetim araçları hakkında bilgi verilir.
- Öğrenci davranışlarıyla ilgili okul-aile iş birliği güçlendirilir.
- Veli bültenlerinde güvenli dijital alışkanlıklar önerileri yer alır.

8. DEĞERLENDİRME VE SÜREKLİ İYİLEŞTİRME

- Politikanın uygulanması yılda bir kez değerlendirme toplantısıyla gözden geçirilir.
- Öğrenci, öğretmen ve veli geri bildirimlerine göre güncelleme yapılır.
- Uygulamada karşılaşılan aksaklıklar için düzeltici-önleyici faaliyetler geliştirilir

9.eGüvenlik POLİTİKAMIZ

eGüvenlik politikası, okulun dijital güvenlik konusundaki kurumsal yaklaşımını, etik ilkelerini ve temel sorumluluklarını belirleyen çerçeve bir belgedir. Öğrencilerin, öğretmenlerin ve velilerin dijital ortamlarda uyması gereken davranış standartlarını ortaya koyar. Ancak bu politikaların uygulanabilir ve sürdürülebilir olması, eGüvenlik Planı ile mümkündür. Plan, politikada tanımlanan ilkeleri somutlaştırarak, okulda alınacak teknik ve pedagojik önlemleri, görev dağılımını ve uygulama adımlarını açıkça belirler.

Bu iki belge bir bütünün tamamlayıcı parçalarıdır: politika yön gösterir, plan ise bu yönün pratikte hayata geçmesini sağlar. Özellikle eTwinning gibi dijital iş birliklerinde güvenli bir eğitim ortamı oluşturmak için politika ve planın uyum içinde geliştirilmesi büyük önem taşır. Bu sayede hem öğrencilerin dijital güvenliği sağlanır hem de okulun teknolojiye karşı kurumsal sorumluluğu sürdürülebilir bir yapıya kavuşur. Okulumuzun web sayfası olan <https://corlusahinleroo.meb.k12.tr/> adresinde eGüvenlik linki içerisinde yayınlanmıştır.

10. SONUÇ

Bu eGüvenlik Okul Güvenlik Planı, öğrencilerin, öğretmenlerin, velilerin ve tüm okul paydaşlarının dijital ortamlarda güvenli, bilinçli ve sorumlu bir biçimde hareket etmesini teşvik etmek amacıyla hazırlanmıştır. Plan kapsamında; teknik güvenlik önlemleri, pedagojik uygulamalar, idari sorumluluklar ve yerel iş birlikleri dikkate alınarak kapsamlı bir güvenlik çerçevesi oluşturulmuştur.

Günümüzde dijital teknolojilerin eğitim süreçlerinde etkin kullanımı kaçınılmazdır. Ancak bu kullanım, ancak gerekli dijital farkındalık, etik değerler ve güvenlik ilkeleriyle desteklendiğinde sağlıklı bir öğrenme ortamı sunabilir. Bu nedenle okul bünyesinde oluşturulan bu plan, sadece bir güvenlik önlemi değil; aynı zamanda dijital vatandaşlık kültürünün gelişmesine yönelik stratejik bir adımdır.

Plan, okul yöneticilerinin liderliğinde; bilişim teknolojileri öğretmenleri, rehberlik servisi, sınıf ve branş öğretmenleri ile velilerin iş birliği içerisinde sürdürülecektir. Öğrencilerin yaş ve gelişim düzeyine uygun içeriklerle desteklenmesi sağlanacak; düzenli ölçme-değerlendirme uygulamalarıyla planın etkililiği gözden geçirilecektir.

Teknolojik gelişmeler doğrultusunda eGüvenlik politikaları dinamik olarak güncellenecek ve gerek ulusal gerekse uluslararası standartlara uyum gözetilecektir. Bu doğrultuda [Okul Adı] olarak dijital güvenlik kültürünü tüm okul topluluğuna benimsetmek ve sürdürülebilir kılmak temel hedefimizdir.

KAYNAKÇA

- Bilgi Teknolojileri ve İletişim Kurumu. (2022). Güvenli internet hizmeti rehberi. <https://guvenliweb.org.tr>
- Bilgi Teknolojileri ve İletişim Kurumu. (n.d.). Çocuklar için bilinçli ve güvenli internet kullanımı el kitabı. <https://guvenliweb.org.tr>
- Kişisel Verileri Koruma Kurumu. (2021). Çocukların kişisel verilerinin korunması rehberi. <https://kvkk.gov.tr>
- Millî Eğitim Bakanlığı. (2022). Bilgi güvenliği politikası ve rehberi. Yenilik ve Eğitim Teknolojileri Genel Müdürlüğü. <https://meb.gov.tr>
- Millî Eğitim Bakanlığı. (2023). 2023–2024 eğitim öğretim yılı eTwinning faaliyetleri rehberi. <https://etwinning.meb.gov.tr>
- Millî Eğitim Bakanlığı. (2018). Bilişim teknolojileri ve yazılım dersi öğretim programı (Ortaokul 5–6. sınıflar). <https://mufredat.meb.gov.tr>
- TÜBİTAK Bilim Genç. (n.d.). Teknoloji ve internet güvenliği yazıları. <https://bilimgenc.tubitak.gov.tr>
- Yeşilay. (2021). Teknoloji bağımlılığı ile mücadele el kitabı. <https://yesilay.org.tr>
- Yeşilay. (2022). Ebeveynler için dijital dünya rehberi. <https://yesilay.org.tr>
- Güvenli Çocuk Platformu. (2021). Dijital dünyada güvenli çocuk olmak: Eğitim içerikleri ve rehber videolar. <https://guvenlicocuk.org>
- T.C. İçişleri Bakanlığı Siberay. (n.d.). Siber güvenlik farkındalık materyalleri. <https://siberay.com>
- Çorlu Bilim ve Sanat Merkezi. (2024). e-Güvenlik uygulama raporu. “Kabul edilebilir kullanım politikası” kapsamında yapılan yerel çalışmalarla öğrenciler ve personel bilinçlendirilmiştir tekirdagarge.meb.gov.tr.
- Tekirdağ İl Emniyet Müdürlüğü Siber Suçlarla Mücadele Şube Müdürlüğü. (2024, 22 Kasım). Tekirdağ’da öğrencilere dijital güvenlik eğitimi [Basın bülteni]. Güvenli internet ve sosyal medya farkındalığı hakkında bilgilendirme yapılmıştır sondakika.com+1tekirdagbakis.com+1.
- Tekirdağ İl Emniyet Müdürlüğü Siber Suçlarla Mücadele Şubesi. (2024, 31 Ekim). Siber güvenlik farkındalık eğitimi [Basın bülteni]. Mesleki teknik lise öğrencilerine yönelik uygulamalı eğitim gerçekleştirilmiştir .
- European Schoolnet. (2021). eSafety label: A review of school eSafety policies. <https://www.esafetylabel.eu>
- ISTE. (2021). ISTE standards for students and educators. International Society for Technology in Education. <https://www.iste.org>
- OECD. (2021). Empowering and protecting children in digital environments. <https://www.oecd.org>
- UNESCO. (2021). Guidelines on digital citizenship education. <https://unesco.org>