



Avrupa Birliği tarafından
finans edilmektedir



Dijital Güvenlik Politikası: Aile ve Çocuk Odaklı Ulusal Strateji

ARALIK 2025

Dijital Güvenlik Politikası: Aile ve Çocuk Odaklı Ulusal Strateji

Aralık 2025

Yayınlayan

ULUM İslami İlimler Eğitim ve Araştırma Merkezi Derneği
Aile ve Toplum Çalışmaları Uygulama ve Araştırma Merkezi
Trabzon Yomra Fen Lisesi
Sosyal Eğitim ve Gelişim Derneği

2025 -I- TR01 -KA154 -YOU- 000300148 kodlu Aile Kurumu ve Dijital Güvenlik projesi Erasmus+ KA154-YOU programı kapsamında Türkiye Ulusal Ajansı tarafından desteklenmektedir. Burada yer alan görüşler yazarların, ortakların görüşlerini yansıtmaktadır. Görüşlerden Avrupa Komisyonu ve Türkiye Ulusal Ajans sorumlu tutulamaz. Yazı ve reklam içerik sorumluluğu sahiplerine aittir. Kaynak gösterilerek alıntı yapılabilir.

Projemizin detaylarına @ulumaileprojesi instagram sayfasından erişebilirsiniz.

Bütün hakları saklıdır.

Giriş

Amaç

Bu politika taslağının amacı, dijital ortamdaki risklere karşı aileleri, çocukları ve ergenleri güçlendirmektir. Bu doğrultuda politika, çevrim içi dünyada karşılaşılan tehditlere karşı önleyici, eğitici ve koruyucu bir yaklaşım geliştirmeyi hedefler. Ayrıca ilgili kurumlar arasında etkin bir koordinasyon sağlamayı ve eğitim, medya, mevzuat, akademik izleme ile uluslararası iş birliklerini tek bir ulusal çerçevede birleştirerek kapsamlı bir dijital güvenlik ekosistemi oluşturmayı amaçlar. Bu sayede, çocukların dijital teknolojiyle sağlıklı etkileşim kurmaları desteklenecek, zarar görme ihtimalleri en aza indirilecektir.

Kapsam

Bu politika aileleri, çocukları ve ergenleri, eğitim kurumlarını, medya ve dijital içerik üreticilerini ve ilgili tüm kamu kurum ve kuruluşlarını kapsar. Toplumun her kesimini, 7'den 70'e tüm yaş gruplarını, dijital dünyadaki riskler ve çözüm yolları konusunda içine alan geniş bir perspektif sunar. Örneğin ebeveynlerden öğretmenlere, gençlik merkezlerinden üniversitelere kadar tüm paydaşlar bu politikanın hedef kitlesidir. Her bir grubun ihtiyaçlarına göre özel stratejiler ve mesajlar geliştirilecektir. Böylece dijital güvenlik kültürü, aile içinde başlayarak okul ve toplum genelinde yaygınlaştırılacaktır.

Dayanak

Politika taslağı 5395, 6284, 2828, 6698 ve 5651 sayılı kanunlar ile BM Çocuk Hakları Sözleşmesi (Genel Yorum No. 25) rehberliğinde hazırlanmıştır. Bu hukuki çerçeve; çocukların ihmalden korunması, aile güvenliği, veri gizliliği ve dijital içerik denetimi konularında devlete yüklenen sorumlulukları temel alır. Politika, dijital güvenlikteki mevcut hukuki mekanizmaları güçlendirmeyi ve çocuk haklarını dijital ortamda tam olarak gözetmeyi hedefler.

Politikanın Gerekçesi: Dijital Risklerin Niteliđi

Dijital teknolojiler ve internet, çocuklar ve gençler için yeni bir yaşam alanı haline gelmiştir. Günümüz çocukları, erken yaşlardan itibaren ekranlarla ve çevrim içi platformlarla büyümektedir. Bu durum, dijital dünyanın faydalarının yanı sıra ciddi riskleri de beraberinde getirmektedir. Siber zorbalık (cyberbullying), dijital bağımlılık (özellikle oyun ve sosyal medya bağımlılığı), mahremiyet ihlalleri (kişisel verilerin kötüye kullanımı, ifşa edilmesi), çevrim içi istismar (ör. çevrim içi ortamlarda çocukların cinsel istismarı, grooming) ve manipölasyon (yalan haber, dezenformasyon, radikalleştirme) gibi olgular, çocuklar açısından yapısal risk alanları oluşturur. Yapay zekâ temelli tehditler de giderek önem kazanmaktadır; örneğın algoritmaların çocuklara zararlı içerikleri önermesi, derin sahte (deepfake) içeriklerle aldatma veya çevrim içi oyunlarda yapay zekânın kumar benzeri dürtüsel harcamaları tetiklemesi bu kapsamdaki yeni risklerdir.

Bu risklerin birçoğı yalnızca bireysel davranışlarla açıklanamayacak kadar çok katmanlı ve sistemiközellikler taşır. Örneğın birçok çevrim içi platformun tasarımı ve iş modeli, kullanıcıları mümkün olduğunca uzun süre çevrim içi tutmaya yöneliktir. Bu da çocukların karşılarına yaşlarına uygun olmayan içeriklerin çıkması ihtimalini artırabilir.

UNICEF tarafından yapılan küresel araştırmalar, çocukların büyük bir bölümünün çevrim içi ortamda gelişim düzeylerine uygun olmayan şiddet veya cinsel içeriklerle karşılaştığını ortaya koymaktadır[2]. Nitekim bir rapora göre gençlerin %62'si internette kendileri için zararlı olabilecek içeriklere maruz kalmıştır[2]. Bir UNICEF anketinde de 25 ülkeden on binlerce gencin %80'i, çevrim içi iletişimin cinsel taciz veya dolandırıcılık riskleri taşıdığını düşündüklerini ifade etmiştir[3]. Bu veriler, gençlerin dijital dünyayı ciddi bir tehdit alanı olarak algıladığını göstermektedir.



Bununla birlikte, dijital risklerin sonuçları yalnız içerikle sınırlı kalmaz; çevrim içi ekran zorbalığı ve taciz vakaları gençlerin psikolojisini derinden etkileyebilmektedir. CDC (ABD Hastalık Kontrol ve Önleme Merkezleri) tarafından toplanan veriler, siber zorbalığa maruz kalan ergenlerde depresyon ve intihar düşüncesi görülme oranının belirgin biçimde arttığını göstermektedir[4]. Araştırmalar, okulda veya internette zorbalık deneyimi yaşayan öğrencilerin intihara teşebbüs etme olasılığının, böyle bir deneyimi olmayan akranlarına göre neredeyse iki katına çıktığını ortaya koymuştur[5]. Bu bulgu son derece kritiktir, zira dijital ortamdaki psikolojik şiddetin gerçek dünyadaki gibi ciddi sonuçlar doğurduğunu gözler önüne sermektedir.

Şekil: Sosyal medya kullanımı ve riskler. CDC'nin 2023 Genç Risk Davranışları araştırmasına göre lise öğrencilerinin %77'si günde birkaç defa sosyal medya kullandığını bildirmiştir. Çok sık sosyal medya kullanan gençler arasında, siber zorbalığa maruz kalma, sürekli üzüntü/umutsuzluk hissetme ve intiharı düşünme oranları anlamlı şekilde daha yüksektir[6]. Bu sonuçlar, dijital platformlardaki tasarım ve algoritmaların gençlerin güvenliğini etkilemede ne denli önemli olduğunu göstermektedir.

Dijital risklerin çok boyutlu doğası, çözümün de bütüncül olmasını gerektirir. Problem, sadece çocukların bireysel tedbirsizliğinden ibaret değildir; platformların tasarım tercihleri, içerik denetleme politikaları, dijital ekonominin çocukları hedef alan reklam ve alışveriş modelleri de riskleri artıran unsurlar arasındadır. Örneğin Avrupa'da yapılan yakın tarihli bir incelemede, birçok çevrim içi oyunun çocukların zayıf yanlarını istismar edecek şekilde tasarlandığı tespit edilmiştir. Oyun içi satın alımlar ve manipülatif tasarımlar ile çocukların kandırılarak para harcamaya yönlendirildiği, şeffaf olmayan uygulamalarla karşılaşıldığı görülmüştür. Bu nedenle Avrupa Komisyonu ve üye ülkeler, video oyun endüstrisinde çocuk tüketicilerin korunmasına yönelik ilkeler benimseyerek oyun tasarımlarının çocukların zayıflıklarını istismar etmemesini vurgulamışlardır[7][8]. Benzer şekilde, Birleşik Krallık'ta çıkarılan Çevrim İçi Güvenlik Yasası uyarınca teknoloji şirketlerine algoritmalarını toksik içerikleri çocuklara önermeyecek şekilde dizayn etmeleri ve çocuklar için güçlü yaş doğrulama mekanizmaları getirmeleri yönünde yükümlülükler getirilmiştir[9][10]. Tüm bu gelişmeler, dijital risklerle mücadelenin çok paydaşlı ve önleyici politikalar gerektirdiğini ortaya koymaktadır.

Özetle, dijital ortam artık çocukların bilişsel, duygusal ve sosyal gelişimini doğrudan etkileyen bir alandır. Çocuklar çevrim içi dünyada öğrenip sosyalleşirken, onları bekleyen tehlikeler de vardır. Bu politika, anılan risklerin farkında olarak, çocukların dijital haklarını koruma ve onların dijital ortamda güvende olma haklarını gerçekleştirme amacını taşımaktadır[1]. Risklerin kapsamı ve ciddiyeti, böylesine kapsamlı bir ulusal politika geliştirilmesini gerekli kılmıştır.





Temel Politika İlkeleri



1. ÖNLEYİCİ YAKLAŞIM

Dijital güvenlik, yalnızca ihlal olduktan sonra cezai tedbirler almakla sağlanamaz. Bu politika, proaktif ve önleyici bir yaklaşımı esas alır. Yani çocukları ve aileleri, dijital risklerle karşılaşmadan önce bilinçlendirmeyi, dijital tehlikelerin erken işaretlerini fark etmelerini sağlamayı hedefler. Örneğin siber zorbalık meydana geldikten sonra müdahale etmek yerine, çocuklara çevrim içi iletişimde saygılı olma ve kendilerini koruma becerileri kazandırmak, önleyici yaklaşımın bir parçasıdır. Bu kapsamda okullarda dijital okuryazarlık eğitimleri, ebeveyn rehberlik programları ve erken uyarı sistemleri (örn. olası bir riskli davranışı tespit eden yazılımlar) devreye sokulacaktır. Amaç, sorun ortaya çıkmadan engelleyebilmektir. Uzmanlar, çocukların çevrim içi risklere karşı dayanıklılığını artırmak için eğitim yoluyla güçlendirmenin, sonradan yaptırım uygulamaktan daha etkili olduğunu vurgulamaktadır



2. AİLE MERKEZLİLİK

Bu politikada aile, dijital dünyada çocuğun en önemli destek mekanizması olarak görülmektedir. Aileler sadece "denetleyici" değil, aynı zamanda rehberlik edici ve koruyucu bir rol üstlenmelidir. Çocukların dijital deneyimlerinde aile ortamının güvenli bir liman olması sağlanacaktır. Politikadaki dil ve ton, aileleri suçlayıcı değil, güçlendirici bir nitelik taşır. Ebeveynlerin dijital konularda bilgi ve farkındalık düzeyi artırılacak, böylece hem kendileri bilinçli internet kullanıcıları olacak hem de çocuklarına doğru rehberlik edebileceklerdir. Örneğin politika kapsamında ebeveynlere yönelik atölye çalışmaları ve kılavuzlar hazırlanarak, çocuklarıyla teknoloji hakkında açık iletişim kurmaları, sınırlar belirlemeleri ve olumlu örnek olmaları teşvik edilir[11]. Araştırmalar, aktif rehberlik yapan ebeveynlerin çocuklarının çevrim içi risklerle daha iyi baş edebildiğini göstermektedir. Kısıtlayıcı ve cezalandırıcı yaklaşımlar yerine, çocuğa güven veren ve birlikte öğrenmeye dayalı yaklaşımlar benimsenecektir. Aile merkezli yaklaşım, dijital güvenliği bir çatışma alanı olmaktan çıkarıp, aile içi işbirliği alanı haline getirmeyi amaçlar.



Temel Politika İlkeleri



3. YAŞ TEMELLİ VE ÇOCUK HAKLARI ODAKLILIK

Çocukluk ve ergenlik dönemleri tek bir kategori olarak ele alınamaz; her yaş grubunun dijital risk profili ve ihtiyaçları farklıdır. Bu politika, gelişimsel farklılıkları dikkate alarak yaşa uygun stratejiler geliştirir. Örneğin ilkökul çağındaki bir çocuk için temel düzeyde güvenli internet kullanımı ve kötü içeriklerden korunma ön plandayken, ergenler için sosyal medyada mahremiyet yönetimi, siber zorbalıkla baş etme ve dijital kimlik konuları öne çıkar. Eğitim içerikleri ve korunma tedbirleri, hedef kitlenin yaşına ve olgunluk düzeyine uyarlanacaktır. Aynı zamanda, tüm çalışmalarda çocuk hakları merkezde tutulur. Çocukların dijital dünyada bilgiye erişim, ifade özgürlüğü, katılım hakkı gibi hakları gözetilirken, özel hayatın gizliliği, korunma ve güvenlik hakları da titizlikle korunacaktır. Birleşmiş Milletler Çocuk Hakları Sözleşmesi'nin dijital ortama uyarlanmasına ilişkin prensipler (BM Çocuk Hakları Komitesi Genel Yorum 25) bu bağlamda yol gösterici olacaktır[1]. Bu ilke, politikanın her adımında "çocuğun üstün yararı" ilkesine uygun hareket edilmesini sağlar.



4. BİLİMSEL DAYANAK VE VERİYE DAYALI UYGULAMA

Politika önerileri ve programlar, bilimsel araştırmalara ve kanıta dayalı yöntemlere dayandırılacaktır. Dijital güvenlik alanı hızla değiştiği için alınan önlemlerin etkinliği düzenli olarak ölçülecek, elde edilen verilere göre politikalar güncellenecektir. Uygulamalar başlamadan önce ön test niteliğinde anketler veya ihtiyaç analizleri yapılacak, uygulama sürecinde düzenli geri bildirim toplanacak ve sonunda son test ile etki değerlendirmesi gerçekleştirilecektir. Elde edilen veriler, hangi programların daha etkili olduğunu, nerelerde iyileştirme gerektiğini gösterecektir. Örneğin bir okuldaki dijital farkındalık eğitimi sonrası öğrencilerin davranışlarında olumlu değişimler olup olmadığı, siber zorbalık vakalarının azalması gibi göstergeler takip edilecektir. Akademik dünya ile iş birliği yapılarak, üniversitelerin bu alandaki çalışmaları politika uygulamalarına entegre edilecektir. Bu sayede politikamız, dinamik bir yapıda, sürekli öğrenen ve kendini geliştiren bir yapıda olacaktır. Bilimsel dayanak ilkesinin bir uzantısı olarak, ulusal ve uluslararası iyi uygulama örnekleri incelenip adapte edilecek; örneğin bir ülkede başarılı olmuş bir dijital vatandaşlık eğitim programı pilot olarak burada da uygulanabilecektir. Sonuç olarak, politika uygulamaları ölçülebilir hedefler etrafında şekillenecek ve sayısal verilerle desteklenen bir yönetim yaklaşımı güdülecektir.



Stratejik Politika Alanları

AİLE VE ÇOCUK FARKINDALIĞI (FABL YAKLAŞIMI)

Aileler, çocuklar ve ergenler için yaş gruplarına özel dijital risk farkındalığı programları geliştirilecektir. Bu çerçevede FABL (Farkındalık ve Bilinçlendirme) yaklaşımı benimsenir. FABL yaklaşımı, dijital risklerin soyut bir kavram olmaktan çıkarılıp günlük yaşamdan örneklerle somutlaştırılmasını sağlar. Örneğin, bir çocuğun çevrim içi bir oyun sırasında yabancı birinden gelen garip bir mesaj alması senaryosu üzerinden siber zorbalık veya çevrim içi istismar tehlikesi anlatılır. Bu yaklaşım kapsamında:

Gündelik yaşam senaryoları: Çocukların ve gençlerin günlük hayatlarında karşılaşılabilecekleri durumlar (ör. bir arkadaşının sosyal medyada dışlayıcı davranması, tanımadığı birinin hediye vaadiyle iletişim kurması gibi) dramatize edilerek farkındalık etkinlikleri düzenlenecek.

Hikâyeleştirme: Dijital riskler masallar, kısa öyküler veya çizgi film karakterleri aracılığıyla özellikle küçük yaş gruplarına uygun şekilde hikâyeleştirilecek. Örneğin, bir "siber kahraman" karakteri aracılığıyla çocuklara internetin güvenli kullanımı eğlenceli biçimde öğretilir.

Görsel ve deneyimsel materyaller: İnteraktif dijital oyunlar, simülasyonlar, çizgi romanlar, posterler ve videolar kullanılarak çocukların dikkatini çekecek materyaller üretilir. Örneğin artırılmış gerçeklik uygulamalarıyla, çocukların yanlışlıkla zararlı bir linke tıklamasının sonuçlarını deneyimleyebileceği güvenli simülasyonlar yapılabilir.

Amaç soyut bir "dijital tehlike" kavramı yerine, çocuğun kendi hayatından kesitlerle özdeşleşebileceği örneklerle öğrenme sağlamaktır.





Stratejik Politika Alanları

EĞİTİM VE KAPASİTE GELİŞTİRME

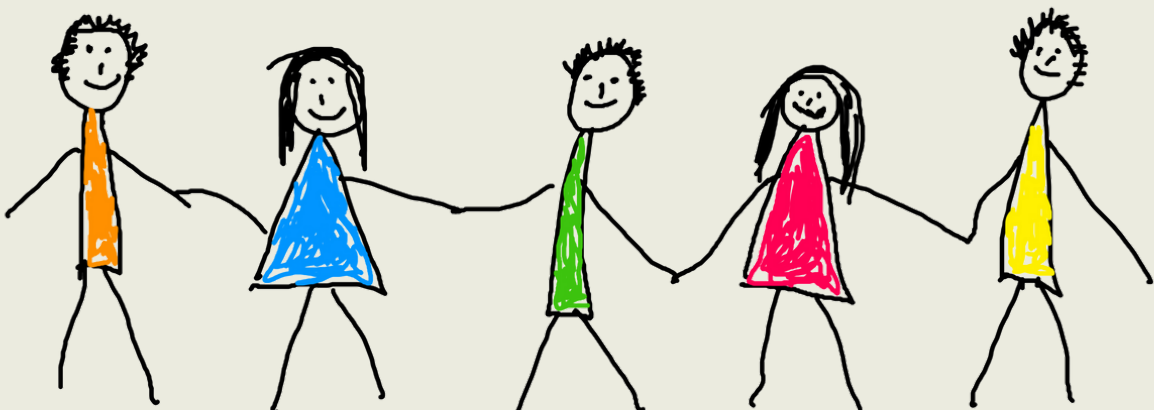
Dijital güvenlik konusunda toplum genelinde kapasite geliştirmek üzere eğitim seferberliği yürütülecektir. Özellikle öğrenciler, veliler, öğretmenler ve rehberlik uzmanları için kademeli eğitim programları hazırlanacaktır. Bu programlar:

Temel, orta ve ileri düzey modüller ile yaş gruplarına ve bilgi düzeyine uygun içerikler sunulacak. Örneğin temel düzeyde ilkokul öğrencilerine “internette güvenli arama nasıl yapılır” öğretilirken, ileri düzeyde lise öğrencilerine “dijital ayak izi ve veri gizliliği” anlatılacaktır.

Yüz yüze eğitimler (okullarda seminerler, halka açık seminerler), çevrim içi eğitimler (e-öğrenme platformları üzerinden interaktif kurslar) ve hibrit eğitimler kombinasyonu ile daha geniş kitlelere ulaşılabilecektir. Özellikle coğrafi olarak dezavantajlı bölgelerde çevrim içi eğitimlerle erişim kolaylaştırılacaktır.

Program içeriği, kısa modüller halinde tasarlanacak (ör. “Siber Zorbalıktan Korunma 101”, “Dijital Oyunlarda Güvenlik”, “Sosyal Medya Etiği” gibi). Bu modüller ihtiyaçlara göre bir araya getirilip esnek şekilde kullanılabilir.

Dijital beceriler ile güvenli kullanım becerileri birlikte ele alınacaktır. Çocuklara kodlama ya da teknoloji üretimi öğretilirken aynı zamanda etik ve güvenlik boyutu vurgulanacaktır. UNICEF, dijital okuryazarlığın günümüzde çocukların eğitim, iş ve hayat becerileri için merkezi bir önem taşıdığını belirtmektedir[12]. Bu doğrultuda politika hem teknik becerileri hem de güvenli kullanım alışkanlıklarını kazandırmayı hedefler.





Stratejik Politika Alanları

MEVZUAT VE KURUMSAL KOORDINASYON

Dijital güvenlik, birçok kurumun sorumluluk alanına giren disiplinler arası bir konudur. Bu nedenle politikanın başarıya ulaşması için açık bir görev dağılımı ve güçlü kurumsal koordinasyon sağlanacaktır. Başlıca görev paylaşımı şöyle öngörülmektedir:

Aile ve Sosyal Hizmetler Bakanlığı: Bu bakanlık, dijital güvenliği aile odaklı bir sosyal risk alanı olarak ele alacak ve lider kurum rolünü üstlenecektir. Ailelerin dijital dünyada karşılaştığı sorunları (ör. dijital şiddet, çevrim içi bağımlılığın aile ilişkilerine etkisi) sosyal hizmet modellerine entegre edecektir. Koruyucu-önleyici sosyal hizmetler kapsamında, örneğin siber zorbalık mağduru çocuklara psikososyal destek sağlanması, teknoloji bağımlılığı riski altındaki çocuklar için danışmanlık hizmetleri sunulması gibi adımlar atılacaktır. Bu bakanlık ayrıca diğer kurumlar arasında koordinasyonu tesis edecek, ulusal düzeyde politikayı yönlendirecektir.

Millî Eğitim Bakanlığı (MEB): Eğitim boyutunun sorumlusu olarak, okullarda uygulanacak programları yürütecek, öğretmen eğitimlerini organize edecek ve müfredat entegrasyonunu sağlayacaktır (yukarıda belirtildiği gibi). MEB, okullardaki ölçme-değerlendirme faaliyetleriyle politikanın etki analizine de katkı sunacaktır.

Radıo ve Televizyon Üst Kurulu (RTÜK): Medya ve dijital içerik denetimi konusunda yetkili kurumdur. RTÜK, televizyon ve isteğe bağılı yayınlarda çocuklara zararlı olabilecek içeriklerin engellenmesi, içerik sağlayıcılara yönelik yaptırımlar gibi mevcut görevlerini dijital platformları da kapsayacak şekilde genişletecektir. Özellikle video paylaşım siteleri, dijital yayın platformları gibi mecralarda çocukların korunması için ulusal düzenlemelerin etkin uygulanması sağlanacaktır. RTÜK ayrıca medya okuryazarlığı kampanyalarında yer alacak, yayıncılara yol gösterici ilkeler belirleyecektir.





Stratejik Politika Alanları

MEVZUAT VE KURUMSAL KOORDINASYON

İletişim Başkanlığı: Kamuoyunu bilgilendirme ve kampanyalar konusunda İletişim Başkanlığı devreye girecektir. Ulusal çapta yürütülecek sosyal kampanyaların, kamu spotlarının ve iletişim stratejilerinin koordinasyonunu yapacaktır. Farkındalık mesajlarının tutarlı ve geniş kitlelere ulaşacak şekilde iletilmesi için medya ile iş birliği içinde çalışacaktır. Ayrıca kriz anlarında (örneğin büyük bir siber zorbalık olayı veya tehlikeli dijital akım yayıldığında) devletin tek bir ağızdan hızlı ve doğru bilgilendirme yapmasını organize edecektir.

BTK (Bilgi Teknolojileri ve İletişim Kurumu) ve ilgili düzenleyici kurumlar: İnternet servis sağlayıcıları, sosyal medya şirketleri gibi özel sektör paydaşlarıyla ilişkilerde ve teknik önlemlerin uygulanmasında rol oynayacaktır. Özellikle 5651 sayılı Kanun çerçevesinde içerik kaldırma, erişim engelleme gibi konularda BTK'nin mevcut yetkileri dahilinde çocukları koruyucu adımlar atılması sağlanacaktır.

UNICEF'in çevrim içi çocuk koruma rehberinde vurguladığı üzere, çocukların dijital ortamda korunması; hükümet, sivil toplum, özel sektör, okul ve aile gibi çok sayıda aktörün birlikte çalışmasını gerektirir[13]. Bu politika tüm bu aktörleri ortak bir vizyon etrafında buluşturmayı hedefler.





Stratejik Politika Alanları

MEDYA VE KAMU İLETİŞİMİ

Dijital güvenlik konusunda toplumsal bilincin artırılması için medya önemli bir araçtır. Bu stratejik alanda, kamuoyu ile etkili iletişim ve medya iş birlikleri ön plana çıkmaktadır. Planlanan adımlar şunlardır:

Kamu Spotları ve Kampanyalar: Televizyon, radyo ve internet platformlarında yayınlanmak üzere, dijital dünyada güvenliğe ilişkin kamu spotları hazırlanacaktır. Bu spotlar, yasaklayıcı değil rehberlik eden bir dil kullanacaktır. Örneğin “şunu yapma, bunu yapma” şeklinde korku veren mesajlardan kaçınılıp, “şöyle yaparsan güvende olursun” şeklinde pozitif ve çözüm odaklı mesajlar verilecektir. Çocukların ilgisini çekmek için çizgi film karakterleri veya ünlü genç idol oyuncular kampanyalara dahil edilebilir. Ebeveynlere yönelik spotlarda ise suçlayıcı üsluptan kaçınılıp destekleyici bir ton benimsenecektir (örn. “Çocuğunuzla internet hakkında konuşun, onu dinleyin” mesajları).

Hedef Kitleye Uygun Dil: Farklı yaş ve kesimler için farklı iletişim diline dikkat edilecektir. Çocuklara yönelik içerikler sade ve eğlenceli olurken, gençlere yönelik kampanyalar akran diline yakın ve interaktif olacaktır. Ebeveynlere yönelik rehber materyallerde ise hem bilimsel bilgiye dayalı hem de pratik öneriler içeren bir yaklaşım kullanılacaktır. Örneğin “Dijital Dünyada Ebeveynlik” adıyla bir rehber e-kitap yayınlanıp ücretsiz dağıtılabilir.

Sosyal Medya ve Influencer İş Birlikleri: Gençlerin yoğun olarak kullandığı Instagram, YouTube, TikTok gibi platformlarda, popüler içerik üreticilerle (influencer’lar) iş birliği yapılacaktır. Bu kişiler aracılığıyla verilecek mesajlar gençler üzerinde daha etkili olabilir. Örneğin sevilen bir YouTuber, kendi kanalında siber zorbalıkla ilgili bilinçlendirme videosu yayınlayabilir veya bir Instagram fenomeni, hikayelerinde güvenli internet ipuçları paylaşabilir. Bu tür iş birliklerinde reklam olduğu şeffafça belirtilerek samimi bir dil tutturulması önemlidir. Aynı zamanda Avrupa Birliği’nin tüketici koruma ilkelerine uygun biçimde, influencer içeriklerinde reklam ve bilinçlendirme mesajlarının ayrımı net yapılacaktır[14].





Stratejik Politika Alanları

MEDYA VE KAMU İLETİŞİMİ

Geleneksel Medya ile İş Birliği: Televizyon dizileri, çocuk programları, çizgi filmler içinde dijital güvenlik temasının işlenmesi teşvik edilecektir. Örneğin bir aile dizisinin senaryosuna, çocuğun siber zorbalık yaşaması ve ailenin bunu çözmesiyle ilgili bir yan hikâye eklenmesi gibi yöntemler, farkındalığı doğal yoldan artırabilir. Yazılı basında uzman görüşleri, köşe yazıları ve röportajlar ile konunun gündemde tutulması sağlanacaktır.

İletişim Başkanlığı ve RTÜK Koordinasyonu: Medya kampanyalarının profesyonel şekilde hayata geçirilmesi için RTÜK ve İletişim Başkanlığı birlikte çalışacaktır. RTÜK, yayıncılarla temas kurarak sosyal sorumluluk projeleri kapsamında destek isteyecek; İletişim Başkanlığı ise mesajların içerik stratejisini belirleyip uygun mecralarda görünürlüğünü takip edecektir. Örneğin belirlenecek bir haftanın "Dijital Güvenlik Haftası" ilan edilmesi ve bu süre boyunca tüm ulusal kanallarda ortak kamu spotları dönmesi sağlanabilir.

Toplumsal Farkındalık Günü: Her yıl Şubat ayında kutlanan Uluslararası Güvenli İnternet Günü (Safe Internet Day) kapsamında ulusal etkinlikler düzenlenebilir. Okullarda bu güne özel programlar, yarışmalar; halka açık paneller; sosyal medyada etiket kampanyaları gibi etkinliklerle toplum genelinde bu konunun önemi vurgulanacaktır.

Bu iletişim stratejileri sayesinde politika mesajlarının geniş kitlelere yayılması ve herkesin kendi rolünü fark etmesi sağlanacaktır. Medya ve iletişim çalışmaları, politikanın görünür yüzü olup hedeflenen kültürel dönüşüm için kritik önemdedir.





GENEL DEĞERLENDİRME

Bu ulusal politika taslağı, dijital güvenliği salt teknik bir mesele olmanın ötesinde, aileyi merkeze alan toplumsal bir güvenlik alanı olarak ele almaktadır. Amaç çocuklarımızı ve gençlerimizi dijital dünyanın zararlarından korurken, onların bu dünyanın sunduğu fırsatlardan da güvenle yararlanabilmelerini sağlamaktır. Politika bir yandan çocukların bilgiye erişim, öğrenme, iletişim kurma gibi dijital haklarını desteklerken, diğer yandan onları istismar, zorbalık, mahremiyet ihlali gibi durumlardan korumak için gerekli önlemleri tanımlamaktadır.

Bu belge, farklı kurum ve kesimlerin ortak bir vizyon etrafında buluşmasını sağlamayı hedefler. Aileler çocuklarıyla sağlıklı bir iletişim kurarak ilk savunma hattı olacak, okullar dijital vatandaşlık becerileri kazandıracak, medya bilinçlendirme rolü üstlenecek, teknoloji şirketleri sorumlu davranacak, yasa uygulayıcılar ve düzenleyiciler ise caydırıcı ve koruyucu önlemleri alacaktır. Hepsinin üzerinde, çocukların üstün yararı ve güvenliği politika yapımının merkezinde tutulacaktır.

Politikanın başarılı uygulanması halinde orta vadede toplumda dijital ortamlara dair bir kültür dönüşümü hedeflenmektedir. Tıpkı trafik güvenliği veya kamu sağlığı konularında olduğu gibi, dijital güvenlik de günlük hayatın doğal bir parçası haline gelmelidir. Ebeveynler çocuklarına nasıl okula giderken “dikkatli ol, yabancılarla konuşma” diyorsa aynı şekilde dijital ortam için de öğütler verebilecek bilinç düzeyine erişmelidir. Çocuklar ve gençler, dijital dünyada karşılaştıkları olumsuzluklarla baş edebilecek dijital dirençlilik geliştirmelidir.

Unutulmamalıdır ki dijital teknolojiler doğru kullanıldığında çocuklar için muazzam fırsatlar sunmaktadır: Eğitimde yenilikler, küresel bilgiye erişim, yaratıcılığın gelişimi, yeni beceriler edinme gibi. Politikamız, çocukları tamamen dijital dünyadan uzaklaştırmak gibi bir yaklaşımı benimsememektedir. Aksine onların bu dünyada güvenli, bilinçli ve etkin bireyler olmalarını desteklemektedir.

Dijital Güvenlik Ulusal Politikası, Türkiye’nin dijital çağda çocuklarını ve ailelerini korumak ve güçlendirmek adına attığı kararlı bir adımdır. Bu politika, içerdiği önleyici tedbirler, eğitim hamleleri, yasal düzenlemeler ve iş birlikleri ile kapsayıcı bir çerçeve sunmaktadır. Başarısı, tüm paydaşların katkısına ve toplumun sahiplenmesine bağlı olacaktır. Hep birlikte çalışarak, çocuklarımız için hem fırsatlarla dolu hem de güvenli bir dijital geleceği inşa edebileceğimize inanıyoruz.



KAYNAKLAR

Bu politika tasarısının hazırlanmasında ulusal mevzuat, UNICEF, WHO, CDC, Avrupa Komisyonu ve çeşitli akademik araştırmalardan yararlanılan bilgiler entegre edilmiştir. İlgili bölümlerde belirtilen kaynaklara ek olarak, “Çocukların Dijital Dünyada Güvenliği” konusunda literatür taraması yapılmış, uluslararası iyi uygulama örnekleri incelenmiştir. Bu sayede politika önerileri sağlam bir bilgi temeline oturtulmuştur. Sonraki aşamalarda da literatürle etkileşim devam edecek, yeni araştırmalar politika uygulamasına yön vermeye devam edecektir.

[1] unicef.org

<https://www.unicef.org/bulgaria/en/media/10596/file>

[2] [11] Harmful content | Parenting | UNICEF Australia

https://www.unicef.org.au/parent-teacher-resources/online-safety/harmful-content?srltid=AfmBOorlAPrMTQEijCgXgosmtoolSgDUmbyaaFg7wRM4ObnS5_vpnpeN

[3] UNICEF: 80 per cent of youth in the world recognize that internet can be a danger

<https://www.unicef.org/kyrgyzstan/press-releases/unicef-80-cent-youth-world-recognize-internet-can-be-danger>

[4] [5] Facts and Support — Megan Meier Foundation

<https://www.meganmeierfoundation.org/facts-and-support>

[6] Frequent Social Media Use and Experiences with Bullying Victimization, Persistent Feelings of Sadness or Hopelessness, and Suicide Risk Among High School Students — Youth Risk Behavior Survey, United States, 2023 | MMWR

<https://www.cdc.gov/mmwr/volumes/73/su/su7304a3.htm>

[7] [8] [14] Social media, online games and search engines - European Commission

https://commission.europa.eu/live-work-travel-eu/consumer-rights-and-complaints/enforcement-consumer-protection/coordinated-actions/social-media-online-games-and-search-engines_en

[9] [10] Tech firms must tame toxic algorithms to protect children online

<https://www.ofcom.org.uk/online-safety/protecting-children/tech-firms-must-tame-toxic-algorithms-to-protect-children-online>

[12] Digital literacy for children: 10 things you need to know - Unicef

<https://www.unicef.org/innocenti/documents/digital-literacy-children-10-things-you-need-know>

[13] [16] [17] unicef.org

<https://www.unicef.org/namibia/media/1341/file/Child%20Online%20Protection%20Factsheet.pdf>

[15] Gaming disorder

<https://www.who.int/standards/classifications/frequently-asked-questions/gaming-disorder>



EKLER

Ek-1: Dijital Risk Türleri – Bu ekte, çocuklar ve gençler için dijital dünyadaki risklerin sınıflandırması sunulmaktadır. İçerik riskleri (zararlı/yaş dışı içerik: şiddet, pornografi, nefret söylemi vb.), iletişim riskleri (çevrim içi ortamlarda kötü niyetli kişilerle temas: grooming, dolandırıcılık girişimleri), davranış riskleri (çocuk ve gençlerin çevrim içi ortamda sergileyebileceği riskli davranışlar: siber zorbalık yapma, aşırı kişisel bilgi paylaşma, müstehcen mesajlaşma gibi) ve ticari riskler (hileli reklamlar, oyun içi satın alma tuzakları, kişisel verilerin izinsiz ticari kullanımı) ana başlıkları altında örneklerle birlikte açıklamalar yer alır. Örneğin, bir çocuk açısından “istenmeyen müstehcen içerik görme” bir içerik riskiyken, “yabancı birinin hediyeyle kandırmaya çalışması” iletişim riski, “başkasına hakaret eden mesaj yazması” davranış riski, “ücretli bir oyunda haberi olmadan aile bütçesini sarsacak harcama yapması” ticari risktir[16][17]. Bu ek, politika kapsamındaki tüm riskleri netleştirerek farkındalık eğitimlerine ve önlem geliştirmeye temel oluşturur.

Ek-2: Kurumsal Rol Dağılım Tablosu – Politikanın uygulanmasında sorumluluk alacak kurumların görev ve sorumluluklarının özetlendiği tablodur. Bakanlıklar (Aile ve Sosyal Hizmetler, Milli Eğitim, Sağlık, Adalet, İçişleri), düzenleyici kurumlar (RTÜK, BTK), yargı organları, yerel yönetimler, okullar, sivil toplum kuruluşları ve özel sektör (sosyal medya platformları, internet servis sağlayıcıları vb.) için ayrı sütunlar halinde “sorumluluklar” listelenir. Örneğin MEB sütununda: “Müfredata dijital güvenlik konularını entegre eder; öğretmen eğitimlerini düzenler; okullarda öğrenci ve veli seminerlerini koordine eder” gibi maddeler bulunur. Adalet Bakanlığı için: “Dijital suçların soruşturma ve yargı süreçlerinde çocuk dostu uygulamalar geliştirir; mağdur çocuklara adli destek sağlar” gibi. Bu tablo, herkesin rolünü bilmesini ve koordinasyonun sağlıklı işlenmesini kolaylaştırır.

Ek-3: Eğitim Modülü Başlıkları – Farklı hedef kitle ve düzeyler için hazırlanmış eğitim modüllerinin listesi verilir. Örneğin:

- “Temel Dijital Okuryazarlık ve Güvenli İnternet” (Öğrenciler için),
- “Siber Zorbalıkla Başa Çıkma Yöntemleri” (Öğrencileri için),
- “Sosyal Medya ve Mahremiyet” (Lise öğrencileri için),
- “Dijital Oyunlar ve Bağımlılık Riskine Karşı Ebeveyn Rehberi” (Ebeveynler için),
- “Öğretmenler için Dijital Vatandaşlık Eğitimi” (Eğitimciler için),
- “Gençler İçin Güvenli Sosyal Medya Kullanımı” (Üniversite degençlik merkezleri için).

Her modülün altında kazanımlar ve kısa içerik özetleri de bulunur. Örneğin “Siber Zorbalıkla Başa Çıkma” modülü kazanımları: öğrenciler siber zorbalığın ne olduğunu tanımlayabilecek, maruz kalırlarsa uygun yardım kanallarını bilecek, tanık olurlarsa nasıl müdahale edeceklerini öğreneceklerdir. Modüller, politika kapsamında standart hale getirilerek ülke genelinde birbiriyle uyumlu eğitimler sağlanacaktır.

Ek-4: FABL Senaryo Türleri – Proje içerisinde oluşturulan örnek FABL senaryoları hazırlanmıştır. Bu sayede daha etkili bir aktarım yapılması sağlanacaktır.



EK 1: DIJITAL RISK TÜRLERİ

Dijital riskler, çocukların ve gençlerin çevrim içi ortamlarda karşılaştıkları psikolojik, sosyal ve fiziksel tehditleri kapsar. Bu riskler literatürde genellikle aşağıdaki başlıklar altında sınıflandırılır:

Risk Türü	Alt Kategoriler	Açıklama	Örnekler
İçerik Riskleri	Şiddet, pornografi, nefret söylemi, dezenformasyon	Yaşa uygun olmayan, zararlı veya travmatik içeriklere maruz kalma	Şiddet içeren videolar, radikal ideolojiler, deepfake içerikler
İletişim Riskleri	Siber zorbalık, grooming (çevrim içi avcılık), taciz	Tanımadığı bireylerle veya akranlarla çevrim içi etkileşim sonucu psikolojik zarar görme	Instagram'da zorbalık mesajları, yabancılarla cinsel içerikli yazışmalar
Davranış Riskleri	Aşırı paylaşım, dijital bağımlılık, kimlik sahteciliği	Çocuğun kendi davranışı nedeniyle karşılaştığı riskler	Sosyal medyada özel bilgilerini paylaşma, oyun bağımlılığı
Ticari Riskler	Manipülatif reklamlar, lootbox, mikro ödeme tuzakları	Dijital ortamda tüketim davranışları yoluyla maddi istismara uğrama	Oyun içi satın almalar, reklama tıklayıp kişisel veri paylaşma
Veri Mahremiyeti Riskleri	İzleme, veri toplama, algoritmik profil çıkarımı	Kişisel verilerin rızasız toplanması ve işlenmesi	Uygulamalar üzerinden konum verisinin paylaşılması
Algoritmik Riskler	Eko odalar, içerik filtreleme, kutuplaştırma	Algoritmaların kullanıcılara gösterdiği içerikler yoluyla görüşlerin daralması	Sadece aynı siyasi görüşte içeriklerin gösterilmesi
Yapay Zekâ Temelli Riskler	Derin sahte içerik (deepfake), sahte hesaplar, önyargılı yapay zekâ	Yapay zekâ sistemlerinin manipülasyon veya yanlış yönlendirme potansiyeli	Deepfake video ile şantaj, çocuk sesi taklidiyle dolandırıcılık
Fiziksel ve Psikolojik Etki	Uyku bozukluğu, dikkat dağınıklığı, ekran bağımlılığı	Dijital cihazların uzun süreli kullanımı sonucu oluşan fizyolojik ve mental etkiler	Yatmadan önce ekran kullanımı sonucu uykuya dalamama, dikkat eksikliği

- UNICEF (2017): Çocukların çevrim içi ortamda en çok karşılaştıkları riskler arasında uygunsuz içerik, kişisel veri ihlali ve siber zorbalık yer almakta.
- OECD (2021): Algoritmik içerik yönlendirmesi, çocukların yalnızca belirli bilgi kaynaklarına maruz kalmalarına neden olabilir.
- WHO: Dijital oyun bağımlılığı, davranışsal bozukluklar sınıfında yer almakta.



EK 2: KURUMSAL ROL DAĞILIM TABLOSU

Kurum / Paydaş	Sorumluluklar
Aile ve Sosyal Hizmetler Bakanlığı	- Ailelere yönelik dijital farkındalık programları geliştirir. - Risk altındaki çocuklara psikososyal destek sağlar. - Çocuk koruma hizmetlerini dijital risklere göre günceller.
Milli Eğitim Bakanlığı (MEB)	- Müfredata dijital güvenlik konularını entegre eder. - Öğretmen eğitimlerini düzenler. - Öğrenci ve veli seminerlerini koordine eder.
Sağlık Bakanlığı	- Dijital bağımlılık ve siber zorbalığa yönelik tedavi hizmetleri sunar. - Sağlık personeli eğitir.
Adalet Bakanlığı	- Dijital suçlarda çocuk dostu yargı süreçleri geliştirir. - Mağdur çocuklara adli destek sağlar.
İçişleri Bakanlığı	- Siber suçlarla mücadeleyi güçlendirir. - Kolluk kuvvetlerini eğitir.
RTÜK	- Çocukları zararlı içeriklerden koruyucu düzenlemeler yapar. - Medya denetimi gerçekleştirir.
BTK	- Güvenli internet hizmetlerini yaygınlaştırır. - Dijital platformları denetler.
Yerel Yönetimler	- Yerel farkındalık faaliyetleri yürütür. - Danışmanlık merkezleri oluşturur.
Sivil Toplum Kuruluşları	- Eğitim ve farkındalık çalışmaları yapar. - Mağdur çocuklara destek verir.
Özel Sektör	- Zararlı içeriklere karşı filtreleme sistemleri kurar. - Kamu ile iş birliği yapar.



EK 3 - MODÜLLER

Modül 1: Temel Dijital Okuryazarlık ve Güvenli Internet

Modülün Amacı

Bu modülün amacı ilkökul öğrencilerinin dijital ortamları güvenli, bilinçli ve sorumlu bir şekilde kullanabilmelerini sağlamak; temel dijital beceriler kazandırarak çevrimiçi risklere karşı farkındalık oluşturmaktır.

Öğrenme Kazanımları

- İnternetin ne olduğunu ve ne amaçla kullanıldığını açıklar.
- Kişisel bilgilerin ne olduğunu ve neden korunması gerektiğini bilir.
- Güvenli şifre oluşturma'nın temel kurallarını öğrenir.
- Tanımadığı kişilerle çevrimiçi ortamda iletişim kurmanın risklerini fark eder.
- Rahatsız edici içerik veya davranışlarla karşılaştığında yardım istemesi gerektiğini bilir.

İçerik Başlıkları

1. İnternet ve Dijital Araçlar Nedir?
2. Güvenli İnternet Kullanımı
3. Kişisel Bilgiler ve Mahremiyet
4. Güçlü ve Güvenli Şifreler
5. Çevrimiçi Oyunlar ve Uygulamalarda Dikkat Edilecek Hususlar
6. Yardım Alma ve Güvenilir Yetişkinler

Uygulama Yöntemleri

- Görsel ve animasyon destekli anlatım
- Sınıf içi soru-cevap etkinlikleri
- Rol oynama ve örnek olay çalışmaları
- Kısa videolar ve etkileşimli içerikler

Süre

Toplam Süre: 4 ders saati

Değerlendirme

Öğrencilerin kazanımları; gözlem formları, sınıf içi etkinlikler ve kısa geri bildirim çalışmaları aracılığıyla değerlendirilir.



EK 3 - MODÜLLER

Modül 2: Siber Zorbalıkla Başa Çıkma Yöntemleri

Modülün Amacı

Bu modülün amacı, ortaokul öğrencilerinin siber zorbalığı tanımasını, bu tür durumlarla karşılaştıklarında doğru ve güvenli şekilde hareket edebilmesini ve dijital ortamlarda saygılı iletişim becerileri geliştirmesini sağlamaktır.

Öğrenme Kazanımları

- Siber zorbalığın ne olduğunu ve türlerini açıklar.
- Siber zorbalığın psikolojik ve sosyal etkilerini fark eder.
- Zorbalıkla karşılaştığında atılması gereken adımları bilir.
- Kanıt toplamanın ve bildirim yapmanın önemini kavrar.
- Dijital ortamda empati ve sorumlu davranış geliştirir.

İçerik Başlıkları

1. Siber Zorbalık Nedir?
2. Siber Zorbalık Türleri
3. Zorbalığın Duygusal ve Sosyal Etkileri
4. Başa Çıkma Stratejileri
5. Kanıt Saklama ve Bildirim Yolları
6. Dijital Empati ve Saygılı İletişim

Uygulama Yöntemleri

- Örnek olay incelemeleri
- Rol oynama etkinlikleri
- Grup çalışmaları ve tartışmalar
- Kısa video ve senaryo analizleri

Süre

Toplam Süre: 4 ders saati

Değerlendirme

Öğrencilerin kazanımları; senaryo temelli değerlendirme, sınıf içi katılım ve kısa yansıtıcı çalışmalar yoluyla ölçülür.



EK 3 - MODÜLLER

Modül 3: Sosyal Medya ve Mahremiyet

Modülün Amacı

Bu modülün amacı lise öğrencilerinin sosyal medyayı bilinçli kullanmalarını, mahremiyetlerini korumalarını, dijital ayak izinin uzun vadeli etkilerini kavramalarını ve çevrimiçi ortamlarda sorumluluk bilinci geliştirmelerini sağlamaktır.

Öğrenme Kazanımları

- Sosyal medyada paylaşılan içeriklerin kalıcı etkilerini açıklar.
- Dijital ayak izi kavramını ve sonuçlarını kavrar.
- Mahremiyet ayarlarını bilinçli şekilde yönetir.
- Çevrimiçi riskleri ve hak ihlallerini tanıır.
- Bilinçli paylaşım ve etik dijital davranış geliştirir.

İçerik Başlıkları

1. Sosyal Medya Kültürü ve Kullanım Alışkanlıkları
2. Dijital Ayak Izi Nedir?
3. Mahremiyet ve Kişisel Veri
4. Sosyal Medyada Riskler ve Hak İhlalleri
5. Paylaşım Öncesi Düşünme Becerisi
6. İtibar Yönetimi ve Dijital Sorumluluk

Uygulama Yöntemleri

- Gerçek yaşamdan örnek olay analizleri
- Tartışma ve grup çalışmaları
- Mahremiyet ayarları uygulamalı gösterimi
- Kısa video ve vaka incelemeleri

Süre

Toplam Süre: 4 ders saati

Değerlendirme

Öğrencilerin kazanımları; örnek olay çözümlemeleri, kısa yazılı yansıtma çalışmaları ve sınıf içi tartışmalar üzerinden değerlendirilir.



EK 3 - MODÜLLER

Modül 4: Dijital Oyunlar ve Bağımlılık Riskine Karşı Ebeveyn Rehberi

Modülün Amacı

Bu modülün amacı, ebeveynlerin dijital oyunların çocuklar üzerindeki etkilerini doğru şekilde değerlendirebilmesini, bağımlılık riskini erken fark etmesini ve ev içinde sağlıklı bir dijital denge kurabilmesini sağlamaktır.

Öğrenme Kazanımları

- Dijital oyunların olumlu ve olumsuz etkilerini ayırt eder.
- Dijital oyun bağımlılığının temel belirtilerini tanır.
- Çocuğun oyun alışkanlıklarını sağlıklı şekilde takip eder.
- Ev içinde dijital sınırlar ve kurallar belirler.
- Çocukla çatışma yerine iletişim temelli yaklaşım geliştirir.

İçerik Başlıkları

1. Dijital Oyunlar: Fırsatlar ve Riskler
2. Oyun Bağımlılığı Nedir?
3. Bağımlılık Belirtileri ve Uyarı İşaretleri
4. Ev İçi Dijital Kurallar ve Zaman Yönetimi
5. Ebeveyn Denetim Araçları
6. Çocukla Sağlıklı İletişim Kurma Yolları

Uygulama Yöntemleri

- Bilgilendirici sunum ve rehber anlatım
- Gerçek yaşam örnekleri üzerinden değerlendirme
- Soru-cevap ve deneyim paylaşımı
- Ebeveyn rehber dokümanları

Süre

Toplam Süre: 2-3 saatlik ebeveyn oturumu

Değerlendirme

Ebeveynlerin kazanımları; geri bildirim formları, öz değerlendirme ve uygulamaya dönük takip çalışmalarıyla değerlendirilir.



EK 4 - FABL VE MASAL SENARYO T RLERİ

RAPUNZEL

Evvel zaman içinde, yüksek ama pencereleri güneşle dolu bir kulede Rapunzel adında bir kız yaşırdı. Bu kule sihirliydi; duvarları konuşmazdı ama pencereleri dünyayı gösterirdi. Rapunzel bu pencerelerden dışarı bakmak yerine, parlak bir aynaya bakmayı severdi. Bu ayna sıradan bir ayna değildi. İçinde renkler, ışıklar ve küçük sihirli dokunuşlar vardı. Rapunzel aynaya gülümsediğinde, ayna onu daha parlak, daha kusursuz gösterirdi.

Rapunzel bu sihirli aynayla konuşur, ona poz verir, saatlerce başından ayrılmazdı. Aynadaki Rapunzel herkesin hayran olduğu bir kızdı. Gerçek Rapunzel ise bazen saçlarını fazla dağınık, yüzünü yeterince güzel bulmazdı. Bu yüzden aynanın süslerini, yani filtrelerini, hep kullanırdı. Zamanla Rapunzel, aynadaki halini gerçek halinden daha çok sevmeye başladı.

Bir gün Rapunzel, kule penceresinden çektiği çok güzel bir görüntüyü aynanın içine bıraktı. Üstelik aynaya kulenin yerini fısıldadı. "Herkes beni buradan görsün," diye düşündü. Oysa aynanın dünyasında sadece iyiler yoktu.

O gün aynanın içinden Gölge Adam geçti. Işığın düştüğü yerlere değil, paylaşılan işaretlere bakardı. Gölge Adam başkalarının bıraktığı izleri takip ederek onları ailelerinden ayırmaya çalışırdı. Rapunzel'in bıraktığı konumu gördü ve kulenin yerini öğrendikten sonra kuleye doğru yol aldı.

Akşam olunca Rapunzel, kule duvarında uzun bir gölge fark etti. Gölge konuşmadı, dokunmadı ama oradaydı. Rapunzel'in içi ürperdi. Hemen ailesinin yanına koştu. Annesi ona sarıldı, babası elini tuttu. "Korku, bazen yanlış açılan bir pencereden girer," dedi babası.

Rapunzel başını eğdi ve Anne babasına, aynaya bıraktığı izleri anlattı. Ailesi ona kızmadı. Ona bir nasihatle bulundular: "Her sihirli ayna güvenli değildir. Sadece bize ait olan ve başkalarıyla paylaşmamamız gereken şeylerde vardır." Rapunzel o gece aynanın süslerini kapattı ve penceresini gerçek dünyaya açtı.

Ertesi sabah Rapunzel, aynaya baktı. Bu kez süs yoktu, filtre yoktu. Sadece kendisi vardı. Kule kapısından aşağı indi, çimenlere bastı, rüzgârı hissetti. Gölge Adam, paylaşılacak bir iz bulamayınca sessizce kayboldu.

O günden sonra Rapunzel aynayı daha dikkatli kullanmayı öğrendi. Nerede, neyi ve kiminle paylaşacağını ailesiyle konuşarak seçti.

Değerlendirme Soruları

- Rapunzel aynaya hangi bilgiyi verdiği için tehlike oluştu?
- Hikâyeye göre herkese her bilgiyi söylemek doğru mudur? Neden?
- sizce anlatılan masalda ayna neyi temsil etmektedir?
- Rapunzel'in yerinde sen olsaydın aynayı nasıl kullanırdın?
- Hikâyeden öğrendiğiniz en önemli ders nedir?



EK 4 - FABL VE MASAL SENARYO TRLERİ

BİTMEYEN OYUN TOHUMU VE POFUDUK

Bir zamanlar yemyeşil bir ormanda Pofuduk adında küçük bir tavşan yaşırdı.

Pofuduk 'un cebinde Bitmeyen Oyun Tohumu vardı.

Bu tohum her dokunulduğunda renkli şekiller çıkarır, yeni oyunlar başlatırdı.

Arkadaşları olan Sincap, kirpi ve kaplumbağa her gün Pofuduk'u oyuna çağırırdı:

"Gel saklambaç oynayalım!"

Ama Pofuduk,

"Bir oyun daha," der ve tohumu bırakamazdı.

Zaman geçti.

Arkadaşları birlikte oynadı, güldü.

Pofuduk ise bir ağacın altında tek başına kaldı.

Akşam olunca annesi yanına geldi:

"Bugün kimlerle oynadın?" diye sordu.

Pofuduk üzgün bir şekilde başını eğdi.

Annesi onun bu halini görünce bütün gün yalnız başına oyun tohumuyla oynadığını anladı.

Ona sarılarak şöyle söyledi:

"Oyun tohumu seni eğlendiriyor ama dostlarını senden uzaklaştırıyor."

Pofuduk düşündü.

Ertesi gün Bitmeyen Oyun Tohumu' nu evde bıraktı ve ormana arkadaşlarının yanına koştu.

Arkadaşlarıyla birlikte zıpladı, oynadı, güldü.

Kalbi çok mutlu oldu.

O günden sonra Pofuduk sihirli tohumla değil, ailesi ve arkadaşlarıyla vakit geçirmeye başladı.

Çünkü şunu öğrendi:

"Oyunlar biter, dostluk kalır."

Değerlendirme Soruları

- Pofuduk neden arkadaşlarıyla oyun oynamıyordu?
- Bitmeyen Oyun Tohumu Pofuduk'un hayatını nasıl etkiledi?
- Pofuduk yalnız kaldığında ne hissetmiş olabilir?
- Sence her oyunun bir sınırı olmalı mı? Neden?
- Pofuduk'un yerinde sen olsaydın ne yapardın?
- Bu hikâyeden çıkarabileceğin en önemli ders nedir?
- Hikâyede oyun tohumu neyi temsil etmektedir



EK 4 - FABL VE MASAL SENARYO TRLERİ

TILKI VE TAVŞAN

Ormanın kenarında, yumuşacık çimenlerin arasında yaşayan küçük bir Tavşan vardı. Bu Tavşan çok meraklıydı. Yeni şeyler öğrenmeyi, farklı sesler duymayı ve ormanda olup bitenleri takip etmeyi severdi. Günlerden bir gün, parlak yapraklarla süslenmiş tuhaf bir duyuru dikkatini çekti. Yaprakların üzerinde altın rengi çizgiler vardı ve şöyle diyordu: “Sana özel, sınırsız havuç bahçesi. Yalnızca seçilen hayvanlar için.”

Tavşan heyecanlandı. “Seçilmiş olabilir miyim?” diye düşündü. O sırada karşısına kibar konuşan, gülümseyen bir Tilki çıktı. Tilki, Tavşan’a ne kadar zeki ve özel olduğunu söyledi. Her cümlesi Tavşan’ın kulağına çok hoş geliyordu. Tilki, bu gizli bahçeye girebilmek için önce Tavşan’ı tanıması gerektiğini söyledi. Nerede yaşadığını sordu, hangi patikadan geçtiğini merak etti. Tavşan bunları anlatırken hiç şüphelenmedi.

Bir süre sonra Tilki, “Bahçenin kapısını açmak için birkaç havuç yeterli,” dedi. Tavşan, ödln çok büyük olduğunu düşünerek havuçlarını verdi. Tilki teşekkür etti, aceleyle uzaklaştı. O günden sonra Tilki bir daha görünmedi. Ne parlak yapraklar kaldı ne de bahçenin izine rastlandı.

Tavşan çok üzüldü. Olanları ailesine anlatınca Anne Tavşan hemen ormanın bilgesi Baykuşu çağırdı. Baykuş, sakın bir sesle Tavşan’a baktı ve şöyle dedi: “Bazı tuzaklar dişlerle değil, güzel sözlerle kurulur. Seni acele ettiren, aileden gizli kalmanı isteyen ve senden bir şey alan herkes iyi niyetli olmayabilir.”

Tavşan başını salladı. Hatasını anladı ama yalnız olmadığını da gördü. Ailesi yanındaydı. O günden sonra Tavşan, anlamadığı hiçbir teklife hemen inanmadı. Bir şey kafasını karıştırdığında önce ailesine sordu. Ormanda yürürken artık sadece ayaklarına değil, sözlere de dikkat ediyordu.

Değerlendirme Soruları

- Tilki, Tavşan’ı kandırmak için hangi sözleri kullandı? Bu sözler sana tanıdık geliyor mu, neden dikkatli olunması gerektiğini düşünüyorsun?
- Tavşan, Tilki ile konuşurken ailesine danışmadı. Sence internette bir teklif aldığımızda bunu ailemizle paylaşmak neden önemlidir?
- Hikâyede Tilki, Tavşan’dan bilgi ve havuç istedi. Gerçek hayatta bir yabancı bizden hangi şeyleri isterse bunun tehlikeli olabileceğini anlayabiliriz?
- Bu hikâyeye göre, internette seni acele ettiren, sır saklamayı isteyen veya senden bir şey talep eden biriyle karşılaşırsan nasıl davranmalısın?

*2025 -1- TR01 -KA154 -YOU- 000300148 kodlu Aile Kurumu ve Dijital
Güvenlik projesi Erasmus+ KA154-YOU programı kapsamında
Türkiye Ulusal Ajansı tarafından desteklenmektedir. Burada yer
alan görüşler yazarların, ortakların görüşlerini yansıtmaktadır.
Görüşlerden Avrupa Komisyonu ve Türkiye Ulusal Ajans sorumlu
tutulamaz.*

Bütün hakları saklıdır.