

13-16 YAŞ ARASI ÇOCUKLARIN EBEVEYNLERİ İÇİN DİJİTAL OKURYAZARLIK VE ÇEVİRİM İÇİ GÜVENLİK REHBERİ

İçindekiler

1. Giriş
2. Adım 1: Dijital Dünyayı Tanıyın
3. Adım 2: Aile İçi İletişim Stratejileri Geliştirin
4. Adım 3: Ekran Süresi ve İçerik Kalitesini Yönetin
5. Adım 4: Sosyal Medyada Güvenlik ve Sınırlar
6. Adım 5: Oyunlar, Lootboxlar ve Oyun İçi Satın Alımlar
7. Adım 6: Yapay Zekâ, Deepfake ve Bilgi Kirliliği
8. Adım 7: Aile Medya Sözleşmesi Oluşturun
9. Kaynakça

Giriş

Dijital dünya, çocuklarımız ve gençlerimiz için eşi benzeri görülmemiş bir evren sunuyor. Bir yanda öğrenme, sosyalleşme, yaratıcılık gibi inanılmaz fırsatlar; diğer yanda ise uygunsuz içerik, siber zorbalık ve bilgi kirliliği gibi ciddi riskler barındırıyor. Bu ikili doğa, sizin gibi pek çok ebeveyni endişelendiriyor. Bu rehberi hazırlamaktaki amacımız korku yaymak değil, sizleri bilinçli ve donanımlı ebeveynler olarak güçlendirmektir. Bu rehber, yasaklar ve katı kurallar yerine, çocuğunuzla aranızdaki diyalogu ve iş birliğini temel alan pratik adımlar sunar. Unutmayın, en etkili koruma kalkanı, çocuğunuzun dijital dünyasını anlama çabanız ve onunla kurduğunuz güven bağıdır.

Bu yolculukta size eşlik etmek ve çocuğunuzun dijital vatandaşlık becerilerini birlikte geliştirmek için buradayız. Gelin, onların dünyasına bir adım atalım ve bu karmaşık ama heyecan verici yolda onlara en iyi nasıl rehberlik edebileceğimizi birlikte keşfedelim.

Dijital Dünyayı Tanıyın

Çocuklarımıza rehberlik edebilmemizin ilk ve en temel adımı, onların zaman geçirdiği dijital dünyanın temel dinamiklerini anlamaktır. Bu, sadece kullandıkları uygulamaları bilmekten öte, bu platformların arka planında nasıl çalıştığını kavramayı gerektirir. Algoritmaların içerikleri nasıl kişiselleştirdiğini, veri toplama mekanizmalarını ve "filtre balonlarının" düşünce yapısını nasıl şekillendirdiğini anladığımızda, çocuklarımızı potansiyel risklere karşı daha etkili bir şekilde koruyabilir ve onlara daha bilinçli bir dijital vatandaş olma yolunda rehberlik edebiliriz.

Gördüklerimiz Neden Farklı?: Algoritmalar ve Kişiselleştirme

Çocuğunuzla aynı anda Instagram veya TikTok akışına baksanız, tamamen farklı içeriklerle karşılaşsınız. Bunun nedeni algoritmalarıdır. Bu platformlar, kullanıcıların hangi videoları izlediğini, hangilerini atladığını, ne kadar süre izlediğini ve hangi içerikleri beğendiğini sürekli olarak kaydeder. Ardından, bu verileri kullanarak her kullanıcıya özel, "beğeneceğini düşündüğü" bir içerik menüsü sunar. Örneğin, çocuğunuz oyun videoları izledikçe, algoritma ona daha fazla oyun videosu önerecektir. Bu "kişiselleştirme" mekanizması, platformların kullanıcıları daha uzun süre ekranda tutmasını sağlar.

Filtre Balonu Nedir?: Yankı Odalarının Etkileri

Algoritmaların sürekli olarak kullanıcının ilgi alanlarına ve mevcut görüşlerine benzer içerikler sunması, zamanla "filtre balonu" (filter bubble) veya "yankı odası" (echo chamber) olarak adlandırılan bir durum yaratır. Gençler, kendilerini hayali bir balonun içinde, sürekli olarak kendileri gibi düşünen ve konuşan insanlarla çevrili bulurlar. Bu durumun birkaç önemli riski vardır ve aslında biz ebeveynler için de geçerlidir:

- **Farklı Görüşlere Karşı Hoşgörüsüzlük:** Sürekli kendi fikirlerinin onaylandığını gören bir genç, farklı bir görüşle karşılaşta daha sert tepki verebilir.
- **Toplumsal Kutuplaşma:** Yankı odaları, insanların karşıt görüşlerle empati kurmasını zorlaştırır ve toplumsal kutuplaşmayı derinleştirir.
- **Sınırlı Dünya Görüşü:** Çocukların ve gençlerin yeni şeyler öğrenme ve farklı kültürleri keşfetme ihtimali azalır, çünkü popüler olan ve zaten sevdikleri şeyler sürekli karşısına çıkar.

Her Tık Bir İz Bırakır: Veri ve Dijital Ayak İzi

Çevrim içi ortamda yapılan her eylem bir iz, yani bir veri bırakır. Bir arama yapmak, bir fotoğrafı beğenmek, bir video izlemek, hatta fare imlecinin hareketi bile kaydedilen birer veridir. Üretilen verinin boyutu ise hayal edilemeyecek kadar büyüktür. Örneğin 2025 yılında bu rehberin yazıldığı zamanda sadece bir dakikada yaklaşık 231 milyon elektronik posta gönderiliyor, 16 milyon mesaj paylaşılıyor ve 5.9 milyon Google araması yapılıyor. Bütün sosyal medya platformlarını ve diğer işlemleri düşündüğünüzde bu devasa veri yığını ne işe yarıyor diye düşünmek gerekiyor. Çünkü bu veriler çeşitli aktörler tarafından toplanır, işlenir ve kullanılır.

- **Markalar:** Ne sevdiğimizi öğrenip ona göre reklamlar ve kampanyalar düzenlerler.
- **Platformlar:** Hangi içeriği bize göstereceklerini belirlemek için algoritmalarını bu verilerle beslerler.
- **Devletler:** Nüfus sayımı, seçim sonuçları ve e-Devlet gibi hizmetleri yönetmek için verilerden faydalanırlar.

Çocuklarımızın (ve belki de bizim) bu dinamikleri anlaması, paylaştıkları her şeyin kalıcı bir dijital ayak izi bıraktığını ve gelecekteki "dijital itibarlarını" şekillendirdiğini kavramaları açısından kritik öneme sahiptir. Çocuğunuzun bıraktığı "dijital ayak izi" (veriler), ona ne göstereceğini belirleyen "algoritmalar" için bir yakıttır. Bu algoritmalar ise zamanla onu farklı fikirlere kapatan bir "filtre balonu" yaratır. Bu görünmez kuralları anlamak, aile içinde sağlıklı bir iletişim kurmanın zeminini hazırlar.

Özetle Dijital Dünyayı Tanımak Neden Önemli

Çocuğunuzun kullandığı platformları, oyunları, uygulamaları ve sosyal medya trendlerini bilmek, riskleri zamanında fark etmenizi sağlar (Common Sense Media, 2024).

Uygulama:

- Çocuğunuzdan sık kullandığı uygulamaları göstermesini isteyin.
- Haftalık "birlikte deneme günü" belirleyin (örneğin birlikte TikTok içeriklerini keşfetmek).

Adım 2: Aile İçi İletişim Stratejileri Geliştirin

Teknik kontroller ve yasaklar, dijital dünyanın karmaşıklığı karşısında tek başına yetersiz kalır. En etkili koruma kalkanı, çocuğunuzla kurduğunuz açık, güvene dayalı ve yargılamadan uzak diyalogdur. Çocuğunuz, çevrim içi ortamda bir sorunla karşılaştığında (siber zorbalık, uygunsuz içerik vb.) size başvurmadan çekinmiyorsa, en büyük adımı atmışsınız demektir. Bu yaklaşım, yasakların getireceği gizlilik ve içe kapanma yerine, sorunları birlikte çözme gücü kazandırır.

Yargılamadan Dinleyin, Anlamaya Çalışın

Unutmayın ki çocuklar ve gençler, dijital dünyayı ve sosyal kuralları bizden çok daha farklı algılayabilir. Bizim için masum görünen bir eylem, onlar için utanç verici bir duruma dönüşebilir. Örneğin bir aile büyüğü, çocuğunun ya da torununun bir maçtaki başarısıyla gurur duyup sosyal medya hesabında "aslanım" diyerek fotoğrafını paylaşabilir. Büyükler için bu bir sevgi ve gurur göstergesiyken, çocuk için bu paylaşım arkadaşları arasında utanç verici ya da alay konusu olabilecek bir duruma dönüşebilir. Bu nesil farkı, iyi niyetli eylemlerin bile nasıl olumsuz sonuçlar doğurabileceğini gösteren mükemmel bir örnektir.

Amacımız yargılamak değil, onların dünyasındaki kuralları ve hassasiyetleri anlamaya çalışmak olmalıdır.

Sorun Anında Sakin Kalın

Bir gün çocuğunuz size gelip uygunsuz bir içerikle karşılaştığını, zorbalığa uğradığını veya bir hata yaptığını anlatabilir. İşte bu an, aranızdaki güven ilişkisinin en kritik testidir.

Vaka Analizi: Bir Güven Testi

13 yaşındaki bir kız, Instagram'da tanımadığı bir yetişkinden uygunsuz fotoğraflar alır. Adam, kendisinden de benzer fotoğraflar göndermesini ister. Kız doğru olanı yapar; adamı engeller, platforma şikâyet eder ve arkadaşlarını uyarır. Ancak ailesine anlatmaktan korkar. Çünkü ailesinin vereceği ilk tepkinin, onu korumak amacıyla Instagram'ı tamamen yasaklamak olacağından emindir. Oysa sorun kızın yaptığı bir şeyde değil, karşıdaki kişinin uygunsuz davranışındadır.

Bu örnekte olduğu gibi, aşırı tepki vermek ve hemen yasaklar koymak, çocuğunuzun bir daha size gelmemeye ve sorunlarını tek başına çözmeye itecektir. Bunun yerine:

- Sakin Kalın:** Panik yapmayın.
- Onu Dinleyin:** Anlattığı için ona teşekkür edin ve ne kadar cesur bir davranış sergilediğini belirtin.
- Güvence Verin:** Suçlu olmadığını, sorunu birlikte çözeceğinizi ve her zaman onun yanında olduğunuzu hissettirin.

Özel Dikkat Gerektiren Durumlar

Her çocuk özeldir ancak bazı gruplar dijital risklere karşı daha savunmasız olabilir. Bu konuda ebeveynlerin daha duyarlı olması önemlidir:

- Göçmen Çocuklar:** Farklı bir ülkeye uyum sağlamaya çalışan gençler için dijital medya, aileleri ve akranlarıyla bağ kurmak için hayati bir araçtır. Ancak, mahrem bilgilerinin (örneğin etnik köken veya göçmenlik statüsü) ifşa olması, onları hedef haline getirebilir.
- Otizm Spektrum Bozukluğu (OSB) Olan Çocuklar:** Sosyal ipuçlarını ve başkalarının niyetlerini anlamakta zorlanabilen OSB'li gençler, kötü niyetli "arkadaşlıklara" ve manipülasyona karşı daha açık olabilirler.
- Engeli Olan Çocuklar:** Toplumda dışlanma ve etiketlenme ile karşılaşabilen engelli gençler, çevrim içi ortamlarda sosyalleşme arayışında olabilirler. Bu durum, onları sanal istismar ve manipülasyona karşı daha hassas hâle getirebilir.

Bu durumlarda, çocuğunuzla daha yakın bir diyalog kurmak ve onların dijital deneyimlerini anlamak her zamankinden daha önemlidir. Güçlü bir iletişim, şimdi ele alacağımız ekran süresi gibi somut kuralları belirlemenin temelini oluşturur.

Açık iletişim, dijital güvenliğin temelidir (FOSI, 2023).

Konuşmayı Başlatmak İçin İpuçları

Diyalog kurmak için sorgulayıcı bir tavır yerine meraklı ve samimi bir yaklaşım benimsemek en doğrusudur. İşte size yardımcı olabilecek bazı açık uçlu sohbet başlatıcıları:

- "Bu aralar en çok hangi oyunları oynuyorsun? Merak ettim, bana da biraz gösterir misin?"
- "İnternette gezinirken seni çok güldüren veya şaşırtan bir şeye denk geldin mi son zamanlarda?"
- "Arkadaşlarınla haberleşmek için en çok hangi uygulamayı kullanıyorsunuz? O uygulamanın en sevdiğiniz yanı ne?"
- "Biliyor musun, ben de internette güvende kalmak için yeni şeyler öğreniyorum. Senin bildiğin ve bana öğretebileceğin ipuçları var mı?"

Uyarı: Cezalandırıcı bir dil, çocukların çevrim içi sorunları saklamasına neden olabilir (Cyberbullying Research Center, 2024).

Adım 3: Ekran Süresi ve İçerik Kalitesini Yönetin

Dijital ebeveynlikte tartışmayı "çocuğum ne kadar süre ekran başında kalmalı?" sorusundan ziyade "ekran başında geçirdiği sürede nasıl bir içerikle etkileşimde bulunuyor?" sorusuna taşımak, modern yaklaşımın temelini oluşturur. Amacımız teknolojiyi bir düşman olarak görüp yasaklamak değil, onu bilinçli, dengeli ve faydalı bir şekilde hayatın bir parçası hâline getirmektir.

Süreden Çok Niteliğe Odaklanın

Tüm ekran süreleri eşit değildir. Çocuğunuzun, çevrim içi aktivitelerini iki ana kategoriye ayırması için teşvik edin:

- Üretken Aktiviteler:** Bunlar, çocuklara ve gençlere yeni bir beceri kazandıran, yaratıcılığını destekleyen veya bilgi dağarcığını genişleten eylemlerdir.
 - Ödev için araştırma yapmak.
 - Kodlama, video düzenleme gibi yeni bir beceri öğrenmek.
 - Bir blog yazmak, dijital müzik yapmak gibi kendi içeriğini üretmek.

-Tüketici Aktiviteler: Bunlar, genellikle pasif bir şekilde içeriğin tüketildiği eylemlerdir.

- Sosyal medyada sadece akışta gezinmek.
- Ardışık olarak kısa videolar izlemek.

Bu ayrımı yapmak hem sizin hem de çocuğunuzun ekran süresini daha anlamlı bir çerçeveye oturtmasına ve "kaliteli" zamana öncelik vermesine yardımcı olur.

Teknik Araçlardan Destek Alın: Ebeveyn Kontrolleri

Açık iletişim en önemli araç olsa da, teknolojik yardımcılar da kuralları uygulamada size destek olabilir. Neredeyse tüm akıllı telefonlar, oyun konsolları (PlayStation, Xbox, Nintendo) ve uygulama mağazaları (Apple App Store, Google Play Store) ücretsiz ebeveyn kontrolü araçları sunar. Bu araçlarla şunları yapabilirsiniz:

- **Yaş Sınırlaması:** PEGI gibi yaş derecelendirmelerine göre çocuğunuzun yaşına uygun olmayan oyun ve uygulamalara erişimini kısıtlayabilirsiniz.
- **Kullanım Süresi Limitleri:** Belirli uygulamalar veya genel cihaz kullanımı için günlük veya haftalık süre sınırları belirleyebilirsiniz.
- **Satın Alımları Engelleme:** Kredi kartınızın izinsiz kullanımını önlemek için uygulama içi satın alımları tamamen engelleyebilir veya bir şifreye bağlayabilirsiniz.
- **Sohbet Kısıtlamaları:** Özellikle oyun konsollarında, çocuğunuzun tanımadığı kişilerle sesli veya yazılı sohbet etmesini kısıtlayabilirsiniz.

Ekran süresini ve içeriğin genel kalitesini yönetmek önemlidir; ancak gençlerin kimliklerini inşa ettikleri ve en yoğun sosyal etkileşimleri yaşadıkları sosyal medya, kendine özgü bir dikkat gerektirir.

Ekran süresi kadar, ne izlendiği de önemlidir (AAP, 2023).

Aksiyon Adımları:

- Günlük ekran süresi hedefi belirleyin.
- Uyku saatinden en az 1 saat önce ekranı kapatın.
- YouTube ve Netflix için "çocuk profili" oluşturun.
- Teknolojisiz alanlar ve zamanlar yaratın.

Adım 4: Sosyal Medyada Güvenlik ve Sınırlar

Sosyal medya, çocuklar için sadece bir eğlence aracı değil, aynı zamanda sosyal kimliklerini inşa ettikleri, akranlarıyla ilişki kurdukları ve kendilerini ifade ettikleri merkezi bir alandır. Bu nedenle, bu alandaki riskleri ve kuralları anlamak ve onlara bu konuda rehberlik etmek kritik bir öneme sahiptir.

Dijital Nezaket Kuralları (Netiket)

Tıpkı gerçek hayattaki gibi, çevrim içi iletişimin de görgü kuralları vardır. "Netiket" olarak adlandırılan bu kurallar, dijital ortamda saygılı ve düşünceli bir iletişim için temel oluşturur. Gençlere öğretmemiz gereken bazı temel netiket kuralları şunlardır:

- **İzin Almak Esastır:** Bir başkasının fotoğrafını veya videosunu, ne kadar masum görünürse görünsün, onun iznini almadan asla paylaşmamak gerekir. Birini bir WhatsApp grubuna eklemeyen önce de mutlaka fikrini sormak önemlidir.
- **Büyük Harflerden Kaçınmak:** Bir mesajın tamamını büyük harflerle yazmak, dijital dilde "BAĞIRMAK" olarak algılanır ve kaba bir davranıştır.
- **Zamanlamaya Dikkat Etmek:** Özellikle geç saatlerde bir arkadaşına mesaj atarken veya görüntülü arama yaparken, "Müsait misin?" diye sormak temel bir nezaket kuralıdır.
- **Gizliliğe Saygı Göstermek:** Bir kişinin size özel olarak gönderdiği bir mesajı, onun izni olmadan başkalarına iletme veya gösterme, güveni ciddi şekilde zedeler.

Mahremiyetin Kalesi: Kişisel Veriler

Çocuklara ve gençlere "Kişisel Veri" kavramını, somut ve anlaşılır bir benzetmeyle anlatabiliriz: "Kişisel bilgilerini korumak, evinin anahtarını veya kimlik kartını tanımadığın birine vermemekle aynı şeydir." Kişisel veri, bir kişiyi tanımlanabilir kılan her türlü bilgidir. Bu sadece T.C. kimlik numarası veya adresle sınırlı değildir. Türkiye'deki Kişisel Verilerin Korunması Kanunu (KVKK) da bu konuya büyük önem vermektedir. Gençlerin bilmesi gerekenler:

- **Fotoğraflar, beğeniler ve konum bilgisi de kişisel veridir.** Bir uygulama indirirken, uygulamanın neden kamera, mikrofon, konum veya telefon rehberi gibi bilgilere erişmek istediğini sorgulamaları gerekir. Bir fotoğraf düzenleme uygulamasının telefon rehberinize erişim istemesi şüphe uyandırmalıdır. Bu izinleri okumadan onaylamak, evinizin anahtarını tanımadığınız birine vermeye benzer.

Kalıcı İzler: Dijital Ayak İzi ve İtibar

İnternetin en önemli kurallarından biri şudur: "İnternet unutmaz." Çevrim içi ortamda paylaşılan her şey (bir yorum, bir fotoğraf, bir video) kalıcı bir dijital ayak izi bırakır. "Sildim" demek, o içeriğin bir başkası tarafından çoktan kopyalanmadığı veya arşivlenmediği anlamına gelmez.

Çocuklara ve gençlere, bugün eğlenceli veya anlık bir hevesle yapılan bir paylaşımın, yıllar sonra bir üniversite veya iş başvurusunda karşılıklarına çıkabileceğini anlatmak önemlidir. Bu, onların dijital itibar kavramını anlamalarını sağlar. Dijital itibar, çevrim içi kimliklerinin bir yansımasıdır ve onu bilinçli bir şekilde inşa etmek, gelecekle için yapacakları önemli bir yatırımdır.

Sosyal medya kadar gençlerin hayatında merkezi bir yer tutan bir diğer alan da kendine özgü ekonomik ve psikolojik dinamikleri olan oyun dünyasıdır.

Mahremiyet ayarları, dijital güvenliğin kilididir (UK Safer Internet Centre, 2025).

Kontrol Listesi:

- Her uygulama için gizlilik ayarlarını birlikte kontrol edin.
- Konum paylaşımı kapalı mı?
- Takipçi listesi tanıdık kişilerden mi oluşuyor?
- Çocuğunuz sizinle paylaşmadan içerik üretiyor mu?

Adım 5: Oyunlar, Lootboxlar ve Oyun İçi Satın Alımlar

Oyun dünyası, pek çok ebeveyn için yabancı bir alan olabilirken, gençler için sosyal etkileşimin, rekabetin ve eğlencenin merkezindedir. Bu dünyanın ekonomik ve psikolojik dinamiklerini anlamak, çocuğunuzun potansiyel risklere karşı korumanıza yardımcı olacaktır.

Ganimet Kutusu (Loot Box) Nedir?

Birçok popüler oyunda bulunan "lootbox" (ganimet kutusu), en basit tanımıyla, içinden ne çıkacağı belli olmayan ve genellikle gerçek parayla satın alınan sanal hazine sandıklarıdır. Bu kutulardan karakter için özel bir kıyafet, daha güçlü bir silah veya nadir bir özellik çıkabilir. Ancak temel mekanizma tamamen şansa dayalıdır. Bu yönüyle, piyango veya kumara benzer bir yapıya sahiptir ve gençleri sürekli harcama yapmaya teşvik edebilir.

Harcamaya İten Psikoloji: FOMO ve Belirsiz

Oyun şirketleri, gençleri daha fazla oyun içi harcama yapmaya yönlendirmek için bazı güçlü psikolojik taktikler kullanır. Bunlardan en yaygın olanları şunlardır:

- **Fırsatı Kaçırma Korkusu (FOMO - Fear of Missing Out):** Bir arkadaşının ganimet kutusundan çok nadir ve havalı bir eşya çıkardığını gören genç, "onlarda var, bende yok" düşüncesiyle kendini dışlanmış hissedebilir. Bu duygu, onu aynı eşyaya sahip olmak için sürekli kutu açmaya itebilir.

- **Belirsizlik ve "Neredeyse Kazanma" Hissi:** Ganimet kutularının şansa dayalı yapısı, beynimizde "bir dahaki sefere kesin çıkar" hissi yaratır. Her açılan kutu, bir sonrakinde büyük ödülü kazanma umudunu besler. Bu belirsizlik, tıpkı kumarda olduğu gibi, kişiyi döngüsel bir harcama davranışına sokabilir.

İçerik Filtresi Olarak PEGI Derecelendirmel

Çocuğunuzun oynadığı oyunların yaşına uygun olup olmadığını anlamanın en pratik yollarından biri, **PEGI (Avrupa Oyun Bilgi Sistemi)** derecelendirmelerini kontrol etmektir. Türkiye'de de geçerli olan bu sistem, ebeveynler için bir yol haritası sunar:

- **Yaş Sınıflandırmaları:** Oyunların ambalajlarında veya dijital mağaza sayfalarında PEGI 3, PEGI 7, PEGI 12, PEGI 16 veya PEGI 18 gibi net yaş derecelendirmeleri bulunur.

- **İçerik Uyarıları:** Bu yaş etiketlerinin yanında, oyunun içeriği hakkında bilgi veren küçük simgeler de yer alır. Bu simgeler; şiddet, kaba dil, korku, kumar veya ayrımcılık gibi unsurların oyunda bulunup bulunmadığını belirtir.

- **Satın Alım Uyarısı:** Ebeveynler için en önemli uyarılardan biri, avuç içi ve kredi kartı simgesiyle gösterilen "Oyun İçi Satın Alımlar" uyarısıdır. Bu simge, oyunun lootbox gibi ek harcama mekanizmaları içerdiğini gösterir.

Oyunlar ve sosyal medya gibi platformlar, aynı zamanda büyük bir bilgi akışının ve maalesef bilgi kirliliğinin de kaynağıdır. Gençleri yeni nesil dijital tehditlere karşı donanımlı hâle getirmek, dijital ebeveynliğin en önemli görevlerinden biridir.

Oyunlar eğlencelidir, ama mali ve psikolojik riskler taşır (BIK, 2023).

Dikkat Edilmesi Gerekenler:

- PEGI yaş derecelendirmelerini inceleyin.
- "Lootbox" içeren oyunlarda harcama sınırı koyun.
- Ortak oyun saatleri belirleyin: birlikte oynayın, tanıyın.

Adım 6: Yapay Zekâ, Deepfake ve Bilgi Kirliliği

Dijital okuryazarlığın en ileri seviyesi, artık sadece insanlar tarafından değil, yapay zekâ tarafından üretilen yanıltıcı içerikleri ve bilgi kirliliğini ayırt etme becerisini gerektiriyor. Çocuklara ve gençlere, dijital dünyada "gördükleri her şeye inanmamaları gerektiğini" öğretmek, günümüzün en hayati derslerinden biridir.

Gördüğüne İnanma: Deepfake (Derin Sahte) Teh

Deepfake (Derin Sahte), yapay zekâ teknolojisi kullanılarak bir kişinin hiç söylemediği şeyleri söylüyormuş veya yapmadığı şeyleri yapıyormuş gibi gösteren, gerçeğinden ayırt edilmesi son derece zor olan sahte videolardır. Bir reklam filminde, hayatını kaybetmiş olan Kemal Sunal'ın canlandırılması bu teknolojinin bilinen bir örneğidir. Bu teknoloji eğlence veya sanat için kullanılabilirdiği gibi, insanları manipüle etmek, sahte haberler yaymak veya birinin itibarına zarar vermek gibi kötü amaçlar için de kullanılabilir. Bu nedenle gençlere, internette gördükleri her içeriğe, özellikle de şok edici veya inanılmaz görünen videolara, şüpheyle yaklaşmaları gerektiğini öğretmeliyiz.

Adım 7: Aile Medya Sözleşmesi Oluşturun

Bu rehber boyunca ele alınan tüm ilkeleri somut ve uygulanabilir bir plana dönüştürmenin en etkili yolu, ailenin tüm üyelerinin katılımıyla bir "Aile Medya Sözleşmesi" hazırlamaktır. Bu belge, katı bir yasak listesi değil; karşılıklı anlayış, ortak sorumluluklar ve dijital dünyada birbirini destekleme taahhüdü içeren bir yol haritası olmalıdır.

Sözleşme Neleri İçermeli?

Her ailenin kendi değerlerine, ihtiyaçlarına ve yaşam tarzına göre özelleştirebileceği bu sözleşmede yer alabilecek temel başlıklar şunlar olabilir:

• Ekran Süresi Kuralları:

- Hafta içi ve hafta sonu günlük kullanım süreleri (dersler ve ödevler hariç).
- Teknolojisiz zaman dilimleri (Örn: Akşam yemeği saatleri, yatmadan 1 saat önce).

• Cihaz Kullanım Alanları:

- Hangi odalarda ekran kullanımının serbest, hangilerinde kısıtlı olacağı (Örn: Yatak odalarında telefon bulundurulmaması).
- Cihazların ortak alanda şarj edilmesi.

• İçerik Türleri ve Kalitesi:

- Yaşa uygun oyun, uygulama ve web sitelerinin birlikte belirlenmesi.
- "Üretken" ve "tüketici" aktiviteler arasında denge kurulması hedefi.

• Mahremiyet ve Paylaşım Kuralları:

- Hangi kişisel bilgilerin (adres, okul adı, telefon numarası vb.) asla paylaşılmayacağını netleştirilmesi.
- Başkalarının fotoğraflarını veya bilgilerini paylaşmadan önce mutlaka izin isteme kuralı.

• Çevrim içi Davranış (Netiket):

- Başkalarına karşı her zaman saygılı ve nazik bir dil kullanılması.
- Siber zorbalığa tanık olduğunda veya maruz kalındığında ne yapılacağı (engelleme, şikayet etme ve bir yetişkine söyleme).

• Güvenlik ve Şifreler:

- Güçlü şifreler oluşturma ve bu şifreleri en yakın arkadaşlarla dahi paylaşmama ilkesi.

• Sorun Anında Başvuru:

- Çevrimiçi ortamda rahatsız edici, kafa karıştırıcı veya korkutucu herhangi bir durumla karşılaşıldığında, sonuçlarından korkmadan derhal ebeveynlere haber verilmesi taahhüdü.

Birlikte Oluşturun ve Esnek Olun

Bu sözleşmenin en önemli özelliği, tepeden inme bir kurallar listesi olmamasıdır. Sürecin başarılı olması için:

• **Müzakere Edin:** Sözleşmeyi hazırlarken çocuğunuzun da fikirlerini alın. Onun görüşlerine değer verdiğinizizi ve makul önerilerini dikkate aldığınızı gösterin. Bu, onun kuralları benimsemesini ve sahiplenmesini sağlar.

• **Esnek Olun:** Bu belge taşa yazılı değildir. Çocuğunuz büyüdükçe, olgunlaştıkça ve daha fazla dijital sorumluluk kazandıkça, sözleşmeyi belirli aralıklarla birlikte gözden geçirin ve güncelleyin.

Dijital ebeveynlik, bir varış noktası değil, teknolojiyle ve çocuğunuzla birlikte sürekli evrilen bir yolculuktur. Bu yolculukta yasaklardan ve korkudan çok; merak, diyalog ve güven en iyi rehberleriniz olacaktır. Çocuğunuzun dijital dünyasını anlamaya çalıştığınızda, ona sadece güvenlik değil, aynı zamanda hayat boyu kullanacağı eleştirel düşünme ve dijital vatandaşlık becerilerini de kazandırabilirsiniz. Bu, onlara verebileceğiniz en değerli armağanlardan biridir.

Sınırlar yazıldığında netleşir (Common Sense Media, 2020).

Sözleşmede Yer Alabilecek Maddeler:

- Hafta içi günlük ekran süresi: dakika
- Sosyal medya paylaşımı onay şartı
- Haftalık Oyun harcama limiti: ...
- Uyumadan önce telefon bırakma saati:
- Cihazlar sadece ortak alanlarda kullanılabilir.

Kaynakça

American Academy of Pediatrics. (2023). Building healthy digital habits. HealthyChildren.org. <https://www.healthychildren.org/English/media/Pages/default.aspx>

Better Internet for Kids. (2023). Guide to online and video games. European Commission. <https://www.betterinternetforkids.eu>

Childnet. (2020). Family agreement. UK Safer Internet Centre. <https://www.childnet.com/resources/family-agreement/>

Common Sense Media. (2020). Family media agreement. <https://www.commonsensemedia.org>

Common Sense Media. (2024). Your 13–16–year–old's digital world. <https://www.commonsensemedia.org>

Cyberbullying Research Center. (2024). Cyberbullying fact sheet: Identification, prevention, and response. <https://cyberbullying.org>

EU Kids Online. (2020). EU Kids Online 2020: Survey results from 19 countries. <http://eprints.lse.ac.uk/103294/>

Family Online Safety Institute. (2023). 7 steps to good digital parenting. <https://www.fosi.org>

National Online Safety. (2022). What parents need to know about deepfakes. <https://nationalonlinesafety.com>

UK Safer Internet Centre. (2025). Advice for parents and carers. <https://saferinternet.org.uk/guide-and-resource/parents-and-carers>

UNESCO. (2021). Media and information literacy: Policy and strategy guidelines. <https://unesdoc.unesco.org/ark:/48223/pf0000377069>

UNICEF. (2020). How to keep your child safe online. <https://www.unicef.org/coronavirus/keep-your-child-safe-online>

Proje kapsamında üretilen senaryo içerikleri kaynak olarak kullanılmıştır.

Yapılandırılmış ve Sınırları Belirgin Anlaşma

Bu şablon, kuralların net olduğu, zaman ve içerik kısıtlamalarının ön planda tutulduğu, daha koruyucu ve "Yapılandırılmış Dijital Ebeveynlik" yaklaşımını benimseyen aileler için tasarlanmıştır.

Alan	Kural ve Sınırlar
I. Cihaz Kullanımı ve Konum (Kısıtlama ve Kontrol)	
Cihaz Konumu 	İnternet erişimi sağlayan tüm cihazlar (bilgisayar, cep telefonu, tablet, oyun konsolu vb.) yatak odaları dışında, ailenin ortak kullanım alanında bulundurulmalıdır.
Zaman Sınırı (Ekran Süresi) 	Çevrim içi geçirilecek toplam süre [saat/gün] olarak net bir şekilde belirlenmeli ve bu süreye sıkı sıkıya bağlı kalınmalıdır. YouTube gibi platformların başında çok fazla zaman geçirme isteğine karşı sınır konulmalıdır.
Cihaz Yapılandırması 	Mobil cihazların ayarları (özellikle küçük çocuklar için) yapılandırılmalıdır; uygulama içi satın alımlar kapatılmalı, yeni uygulama kurulması engellenmeli ve yer konumlaması/GPS kullanımı hizmet dışı bırakılmalıdır. Yönlendiricinin (router) güvenlik ayarları da kontrol edilmelidir.
Harcama Yönetimi 	Mali durumları sorumlu bir şekilde yönetemeyen küçükler için aylık abonelik yerine "ön ödemeli" planlar tercih edilmelidir; harcamalar tartışılmalı ve paranın gerçek değeri anlaşılmalıdır. Uygulama içi satın alımlar (oyunlarda dahi) kontrol edilmelidir.
Alan	
II. İçerik ve Güvenlik (Filtreleme ve Denetim)	
Ebeveyn Denetimi 	Zararlı içerikleri engellemek için internet filtreleri, ebeveyn kontrol uygulamaları (Örn: Güvenli İnternet Hizmeti) veya filtrelenmiş arama motorları kullanılmalıdır. Beyaz listeler oluşturularak çocukların onaylanmış sitelere hızlı erişmesi sağlanmalıdır.
Yazılım Güvenliği 	Kullanılan her cihazda anti-virüs filtresi ve kötü amaçlı yazılım koruması yüklü olmalı ve güncel tutulmalıdır.
Sosyal Medya ve İzleme 	Çocuğun sosyal medya hesapları, ziyaret ettiği siteler ve uygulamalar ebeveyn tarafından düzenli olarak takip ve kontrol edilmelidir. Çocuklar tarafından kullanılan cihazlara "misafir" hesaplar oluşturulmalıdır.

Alan	Kural ve Sınırlar
III. Kurallar ve Yaptırımlar (Netlik ve Tutarlılık)	
Şifre Paylaşımı	 <p>Çocuğun kullandığı tüm şifre/parolalar ebeveynler dışında kimseyle paylaşılmamalıdır; ebeveynler bu şifreleri bilmelidir. Kolayca tahmin edilemeyecek şifreler belirlenmelidir.</p>
Hukuki Sorumluluk	 <p>İnternette bireylerin kişisel bilgilerini ele geçirmeye çalışmak, taciz veya tehdit etmek gibi davranışların suç olduğu bilinmeli ve bu durumlarda aile ile birlikte yasal yollara başvurulmalıdır.</p>
Kural İhlali Durumları	 <p>Kuralların ihlali durumunda uygulanacak yaptırımlar (ekran süresi kısıtlaması, cihazı geçici süreyle alma vb.) açıkça belirlenmeli ve tutarlı olunmalıdır. Ancak çocuk cihazını disiplin önlemi olarak elinden alma konusunda dikkatli olunmalıdır.</p>

Yapılandırılmış ve Sınırları Belirgin Takvim (Zaman Kısıtlaması Odaklı)

Bu takvim, ekran süreni kontrol etmeni ve günlük kullanımını düzenlemene yardımcı olmak için hazırlanmıştır. Şimdi, bu takvimi nasıl uygulayacağını adım adım inceleyelim.

- Her gün için izin verilen azami ekran süresi tabloda yazıyor. Bu süreyi ödev, araştırma, oyun veya eğlence için kullanabilirsin.
- Gün sonunda kaç dakika ekran kullandığını tabloya işaretle.
- Ekranı hangi amaçla kullandığını kısa bir şekilde yaz (örneğin: "ödev", "dizi", "araştırma", "oyun").
- Günü tamamladığında kendin veya ailen tabloyu "Onay" bölümünden işaretle.
- "Notlar" kısmına
 - kurallara uyup uymadığını,
 - hangi gün daha fazla/daha az ekran kullandığını yazabilirsin.

Gün	Belirlenen Azami Süre (Saat: Dakika)	Kullanım Amacı (Örn: Ödev, Eğitim, Oyun)	Harcanan Gerçek Süre (Saat: Dakika)	Onay (Ebeveyn veya Öğrenci)	Notlar (Kurala Uyuldu mu?)
Pazartesi	[Örn: 1:30]				
Salı	[Örn: 1:30]				
Çarşamba	[Örn: 1:30]				
Perşembe	[Örn: 1:30]				
Cuma	[Örn: 2:00]				
Cumartesi	[Örn: 2:30]				
Pazar	[Örn: 2:30]				
Haftalık Toplam	[Haftalık Limit]		[Toplam Harcanan]		

Kurallar ve Değerlendirme

- İlave Süre:** Belirlenen azami süre aşıldığında [Yaptırım: örn: ertesi gün 30 dakika kesinti] uygulanacaktır.
- Cihaz Kullanım Alanı:** Cihazlar yatak odası dışında, ortak kullanım alanında kullanılacaktır.
- Haftalık Kontrol:** Hafta sonunda harcanan toplam süre, izin verilen haftalık sınır ile karşılaştırılacaktır.
- Uygulama İzinleri:** Yalnızca ebeveyn onayı ile belirlenen uygulamalar/oyunlar kullanılacaktır.

İş Birliğine Dayalı ve Esnek Takvim (Denge ve Amaç Odaklı)

Bu form, internette geçirdiğin zamanı daha bilinçli kullanmana ve çevrim dışı etkinliklerle dengede tutmana yardımcı olmak için hazırlanmıştır. Aşağıdaki maddeler, formu doldururken sana yol gösterir:

- Her gün internette hangi uygulamaları ya da platformları kullandığını forma yaz.
- O gün ekranda ne kadar zaman geçirdiğini dakika olarak belirt.
- Çevrim içi zamanı hangi amaçla kullandığını yaz. Örneğin: bilgi edinme, ödev yapma, yaratıcı bir şey üretme, oyun oynama, arkadaşlarıyla iletişim kurma.
- Gün içinde yaptığın çevrim dışı etkinlikleri ekle. Bu; spor, kitap okuma, aile zamanı, oyun oynama, yürüyüş gibi etkinlikler olabilir.
- Hafta sonunda toplam sürelerine bakarak kendini değerlendir: Ne kadar çevrim içi ne kadar çevrimdışı zaman geçirdin?
- Formu haftanın sonunda ebeveyninle birlikte gözden geçirerek neleri iyi yaptığını ve neleri geliştirebileceğini konuş.

Gün	Kullanılan Platform/Uygulama	Harcanan Süre (Dakika)	Kullanımın Amacı (Örn: Bilgi, Yaratıcılık, Sosyalleşme, Eğlence)	Dengelenen Çevrimdışı Faaliyetler (Örn: Spor/Kitap/Aile Zamanı)
Pazartesi	[Örn: YouTube Kids / MOOC]	[Örn: 45 dk]	Bilgi arama (Ödev)	30 dk Aile zamanı (Çevrim dışı)
Salı	[Örn: Çevrim içi Oyun (MMOG) / Sosyal Medya]	[Örn: 60 dk]	Sosyalleşme Eğlence	45 dk spor faaliyeti
Çarşamba	[Örn: Blog / Vlog hazırlama]	[Örn: 90 dk]	Yaratıcılık	60 dk spor faaliyeti
Perşembe				
Cuma				
Cumartesi				
Pazar				
Haftalık Toplam	[Tanınan Süre / Harcanan Süre]			[Toplam Çevrimdışı Süre]

Taahhütler ve Gözden Geçirme

- Haftalık Bütçe:** Bana bu hafta harcayabileceğim [toplam x saat] çevrim içi süre tanınmıştır. Süremi sorumlu bir şekilde yönetmeyi taahhüt ediyorum.
- Amaç Odaklılık:** Çevrim içi sürenin bir iş modeli ve para birimi olduğunu anlıyorum. Çevrim içi zamanımı öğrenme, yaratma ve olumlu yollarla bağlantı kurma etkinliklerini içerecek şekilde dengeleyeceğim.
- Değerlendirme:** Hafta sonunda bu formu ebeveynimle birlikte gözden geçireceğim (Diyalog, filtreleme güvenmekten daha önemlidir). Eğer kötü bir içerikle karşılaşsam veya zor durumda kalırsam, hemen güvenilir bir yetişkine haber vereceğimi taahhüt ederim.

Emojilerle Duyguları İfade Etme Çalışması

Dijital Mesajların İçerdiği Duyguyu Anlama

Adı Soyadı:

Tarih:

Aşağıdaki mesajları okuyun ve her birinin, emoji olmadan ve emoji ile birlikte size hangi duyguyu hissettirdiğini işaretleyin.

Mesaj	Emoji Yoksa Hissedilen Duygu (Örn: Öfke/Kafa Karışıklığı)	Kullanılan Emoji	Emoji Varsa Hissedilen Duygu (Örn: Eğlence/Mizah)
1. "Yaptığın şey çok saçmaydı."		😞	
2. "Bu kadar uzun süre çevrim içi olman doğru değil."		😞	
3. "Yarınki sunum için yardım etmen gerek."		🙏	
4. "Profilini neden herkese açık yaptın? Bu riskli."		😞	
5. "Bu ödev için en iyisi bu site."		👍	

Netiquette (Ağ Etik Kuralları) Kuralı

Bir sohbet odasında veya sosyal medyada nazik ve uyumlu bir mesaj göndermek için hangi duygu ikonlarını, neden kullanmalıyız? Cevabınızı bir arkadaşınıza açıklayacak şekilde yazınız.

Cevabım:

Mesaj gönderirken emoji kullanırım çünkü yazdığım şeyin nasıl hissettirdiğini daha açık göstermek isterim. 😊 Sadece yazı bazen yanlış anlaşılabilir 😞 ama emoji ekleyince niyetimi daha iyi anlatırım. 💬 Böylece karşımdaki kişi alınmaz, üzülmez ya da beni yanlış anlamaz. 🧑🧑 Emoji kullanmak dijital ortamda nazik, uyumlu ve iyi huylu olmamı sağlar.



Yapılandırılmış ve Sınırları Belirgin Anlaşma

Bu şablon, diyalog kurmayı ve ortak karar almayı teşvik eden, sorumluluk, rehberlik ve dijital dayanaklılık geliştirmeyi amaçlayan aileler için tasarlanmıştır.

Alan	Rehberlik ve İş Birliği Taahhütleri
I. Diyalog ve Güven (İletişim ve Destek)	
Açık İletişim Hattı 	<p>Çocuklarla düzenli, dürüst ve açık bir diyalog kurulmalı ve çevrim içi deneyimleri hakkında konuşulmalıdır.</p> <p>Çocuğun her şeyi ebeveyniyle konuşabileceği güvenli bir ortam sağlanmalıdır, eleştirel ve yargılayıcı bir tutumdan kaçınılmalıdır.</p>
Rol Model Olma 	<p>Ebeveynler kendi teknoloji kullarımlarına sınır koyarak çevrim içi davranışlarıyla olumlu bir dijital rol model olmalıdır.</p>
Yardım Mekanizmaları 	<p>Çocuk, çevrim içi bir sorunla karşılaştığında (zorbalık, uygunsuz içerik vb.) kimden yardım alacağını (ebeveyn, öğretmen, güvenilir yetişkin, ulusal yardım hattı) bilmeli ve yardım istemekten çekinmemelidir. Çocuğa, saldırgan bir içerikle karşılaştığında cihazı kapatma ve güvenilir bir yetişkine bildirme yolları öğretilmelidir.</p>
Alan	Kural ve Sınırlar
II. Dijital Vatandaşlık ve Sorumluluk (Eğitim ve Empati)	
Kişisel Bilgi Yönetimi 	<p>Çocuklar, kişisel bilgilerini (ad, adres, okul, konum, özel fotoğraf/video) paylaşmamaları gerektiğini ve bunun uzun vadeli sonuçları olabileceğini anlamalıdır. Profil oluştururken kişisel olmayan görseller kullanılmalıdır.</p>
Eleştirel Düşünme 	<p>Çocuklar, internette gördükleri bilgilerin doğruluğunu sorgulamaya ve manipülasyonlara (deepfake vb.) karşı dikkatli olmaya teşvik edilmelidir.</p>
İtibar ve Kalıcılık 	<p>Yazılan, gönderilen veya paylaşılan her şeyin internet üzerinde süresiz olarak kalabileceği, değiştirilebileceği ve başkalarına gönderilebileceği hatırlatılmalıdır. Çevrim içi itibarın yönetilmesi gerektiği öğretilmelidir.</p>
İzinsiz Paylaşım Yasağı 	<p>Çocukların veya başkalarının kişisel bilgileri veya fotoğrafları izinleri olmadan çevrim içi olarak paylaşılmamalıdır.</p>

Alan	Kural ve Sınırlar
III. Esneklik ve Ortak Öğrenme (Gelişim ve Denge)	
Birlikte Öğrenme 	Çocukların çevrim içi deneyimleri hakkında tartışmayı teşvik etmek ve güvenlerini artırmak amacıyla ebeveynler mümkün olduğunca yanlarında kalmalı ve birlikte öğrenmek için fırsatlar yaratmalıdır. Ebeveynler, çocukların kullandığı uygulamaları kendileri de deneyimlemelidir.
Denge 	İnternet kullanımı ve ekran süresi ile ilgili sağlıklı bir denge bulunmalıdır. Çevrimdışı aile zamanının önemi vurgulanmalı ve sportif/sosyal faaliyetlere vakit ayrılmalıdır.
Dijital Dayanıklılık Geliştirme 	Çocuklar, olumsuz deneyimlerden (siber zorbalık vb.) sonra iyileşme ve öğrenme yolları bulmaları konusunda desteklenmeli, böylece dijital dayanıklılık geliştirmeleri sağlanmalıdır.
Yabancılarla İletişim 	Çevrim içi tanışılan biriyle fiziki buluşma kararı verilmeden önce mutlaka ebeveyne söylenmeli ve güvenilir bir yetişkin eşliğinde, halka açık yerlerde buluşulmalıdır. Tanınmayan kişilerden gelen arkadaşlık teklifleri kabul edilmemelidir.

Gizlilik ve Güvenlik

<p>RİSK: Zayıf ve Tahmin Edilebilir Şifreler</p> <p>123456 gibi zayıf ve tahmin edilebilir şifreler saniyeler içinde kırılabilir ve hesapların çalınmasına yol açabilir.</p>	<p>İPUCU: Güçlü Koruma Kalkanları Oluşturun</p> <p>Uzun ve karmaşık şifreler kullanın, her hesap için farklı bir şifre belirleyin ve İki Aşamalı Doğrulamayı (2FA) etkinleştirin.</p>
<p>RİSK: Kişisel Bilgilerin Paylaşılması</p> <p>Adres, okul, telefon numarası gibi bilgiler kötü niyetli kişiler tarafından kullanılabilir</p>	<p>İPUCU: Dijital Mahremiyet Bilinci Kazandırın</p> <p>Çocuğunuza özel bilgilerin internette tanımadığı kişilerle asla paylaşılmaması gerektiğini öğretin.</p>

Sosyal Medya

<p>RİSK: Kalıcı Dijital Ayak İzleri ve "Sharenting"</p> <p>İnternette paylaşılan her şey kalıcıdır ve gelecekte çocuğun karşısına çıkabilir. Ayrıca sharenting denilen ebeveynlerin paylaşımı da bir risktir.</p>	<p>İPUCU: Bilinçli Paylaşım ve Rol Model Olma</p> <p>Çocuğunuzun özel fotoğraflarını ve bilgilerini paylaşmaktan kaçının. Sosyal medya hesaplarında gizlilik ayarlarını birlikte yapın.</p>
<p>RİSK: Yanlış Bilgi ve Tık Tuzakları</p> <p>Sosyal medyada hızla yayılan yalan haberler (dezenformasyon) ve merak uyandıran başlıklar zararlı içeriklere yönlendirebilir.</p>	<p>İPUCU: Eleştirel Düşünmeyi Öğretin: Dur, Düşün, Paylaş!</p> <p>Karşılaştığı her bilgiyi sorgulamasını, kaynağını kontrol etmesini ve doğrulamadan paylaşmamasını telkin edin.</p>

Siber Zorbalık

<p>RİSK: Sanal Dünyanın Acımasız Yüzü</p> <p>Alay etme, dışlama, tehdit veya aşağılayıcı içerikleri yayınlama gibi davranışlar çocuklarda derin psikolojik yaralar açar.</p> <p>RİSK: Dijital Linç ve Sürü Psikolojisi</p>	<p>İPUCU: Sakin Kalın, Dinleyin ve Kanıt Toplayın</p> <p>Çocuğunuza güven verin, durumu anlatmasını sağlayın. Mesajların ekran görüntüsünü alın ve zorbalık yapan hesabı engelleyip şikâyet edin.</p> <p>İPUCU: Empatiyi Teşvik Edin</p>
<p>Olayın aslını bilmeden bir kişiye karşı toplu saldırılar, masum birinin bile büyük zarar görmesine neden olabilir.</p>	<p>"Bu sana yapılırdı ne hissederdin?" sorusunu sorarak çocuğunuzu başkalarının yerine kendini koyma becerisini geliştirin.</p>

Yapay Zekâ (AI)

<p>RİSK: Aşırı Bağımlılık ve Düşünme Tembelliği</p> <p>Her kararı yapay zekaya sormak, çocukların eleştirel düşünme ve problem çözme yeteneklerini zayıflatır.</p>	<p>İPUCU: Yapay Zekâyı Karar Verici Değil, Araç Olarak Kullanın</p> <p>"Bot değil, beyin sensin" mottosuyla çocuğunuzu kendi fikirlerini oluşturmaya, yapay zekâdan aldığı bilgiyi başka kaynaklardan kontrol etmeye teşvik edin.</p>
<p>RİSK: Gizli Veri Toplama</p> <p>Yapay zekâyâ sorulan kişisel sorular ve kararlar sunucularda depolanır ve kötüye kullanılabilir.</p>	<p>İPUCU: Özel Bilgileri Yapay Zekâdan Uzak Tutun</p> <p>Çocuğunuza hassas kişisel bilgilerini ve özel sırlarını yapay zekâ sohbet robotlarıyla paylaşmaması gerektiğini öğretin.</p>

Dijital Oyunlar

<p>RİSK: Kontrolsüz Oyun İçi Harcamalar</p> <p>"Ganimet sandıkları" (lootbox) ve uygulama içi satın alımlar, farkında olmadan yüksek maliyetlere yol açabilir.</p>	<p>İPUCU: Ebeveyn Kontrolleri ve Aile Kuralları Belirleyin</p> <p>Cihazlardan oyun içi satın alımları kısıtlayın veya şifreye bağlayın. Harcama limitleri hakkında net kurallar koyun.</p>
<p>RİSK: Yabancılarla Sohbet ve Uygunsuz İçerik</p> <p>Oyun içi sohbetler siber zorbalığa, kötü niyetli yetişkinlerle temasa ve yaşa uygun olmayan konuşmalara zemin hazırlayabilir.</p>	<p>İPUCU: Yaş Sınırlarına Uyun ve Birlikte Oynayın</p> <p>Oyunların yaş derecelendirmelerini (PEGI vb) kontrol edin. Oyunu birlikte oynayarak hem içeriği denetleyin hem de çocuğunuzla iletişim kurun.</p>

Öğrencinin Kendi Dijital Davranışlarını Değerlendirme Formu

Aşağıda, dijital güvenlik, mahremiyet, dijital vatandaşlık ve çevrim içi öğrenme davranışlarını içeren kısa ifadeler yer almaktadır.

Bu form, sizin günlük dijital davranışlarınızı ne ölçüde gerçekleştirdiğinizi kendi kendinize değerlendirmenizi amaçlamaktadır.

Lütfen her maddeyi dikkatlice okuyarak, sizi en doğru yansıtan seçeneği işaretleyiniz.

Değerlendirme Ölçeği

3 = Her Zaman

2 = Bazen

1 = Hiç

Formu Doldururken Dikkat Etmeniz Gerekenler

- ✓ İlk aklınıza gelen doğal davranışınızı temel alınız.
- ✓ Çevrenizin beklentilerini değil, gerçek dijital davranışlarınızı yansıtınız.
- ✓ Bu formda doğru –yanlış cevap yoktur; önemli olan dürüst ve kendinize uygun bir değerlendirme yapmanızdır.
- ✓ Hiçbir maddeyi boş bırakmayınız.
- ✓ Verdiğiniz bilgiler yalnızca eğitsel geri bildirim amacıyla kullanılacaktır.

Puanlama ve Yorumlama

Her bölümdeki maddeleri cevapladıktan sonra, toplam puanınız hesaplanacaktır.

Toplam puan, dijital güvenlik, mahremiyet bilinci, çevrimiçi davranışlar ve siber zorbalıkla baş etme becerileriniz hakkında genel bir değerlendirme sunar.

Adı Soyadı:

Tarih:

Bölüm 1: Dijital Güvenlik ve Cihaz Yönetimi

Davranış İfadesi	1- Her Zaman	2- Bazen	3- Hiç
1. Hesaplarım için güçlü, kolay tahmin edilemeyen (doğum tarihi, isim vb. içermeyen) şifreler belirlerim.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
2. Şifrelerimi (e -posta, sosyal medya, oyun) kimseyle paylaşmam.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
3. Başka cihazlarda veya bilgisayarlarda işim bittiğinde hesabımdan çıkış yapar ve bilgilerimin kaydolmadığından emin olurum.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
4. Cihazlarımda (telefon, tablet, bilgisayar) virüs ve kötü amaçlı yazılımları engelleyici programlar (anti -virüs filtresi) kullanırım ve güncel tutarım.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
5. Uygulama indirirken (oyun dahi olsa) uygulama izinlerini okur ve gereksiz izinleri (kamera, rehber, konum gibi) vermem.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Bölüm 2: Dijital Mahremiyet ve İtibar Yönetimi

Davranış İfadesi	1- Her Zaman	2- Bazen	3- Hiç
6. Çevrimiçi ortamlarda açık adresim, okul adım, telefon numaram gibi kişisel bilgilerimi paylaşmam.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
7. Kendi paylaştığım veya başkalarının benimle ilgili paylaştığı içeriklerin (fotoğraf, yazı, video) internette sonsuza kadar kalabileceğini aklımda tutarım.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
8. Sosyal medya veya oyun hesaplarımın gizlilik ayarlarını (kimlerin içeriğimi görebileceği vb.) düzenli olarak kontrol eder ve yönetirim.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
9. Arkadaşlarıma veya tanıdıklarına ait fotoğraf veya videoları, onların izni olmadan çevrimiçi paylaşmam.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
10. Çevrimiçi paylaşımlarımdan önce, okulun/ailemin internet güvenlik politikasını veya kurallarını düşünürüm.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Bölüm 3: Dijital Vatandaşlık ve Zorbalıkla Mücadele

Davranış İfadesi	1- Her Zaman	2- Bazen	3- Hiç
11. Çevrimiçi ortamlarda (oyun sohbeti, mesajlaşma, yorumlar) her zaman saygılı, açık ve sağlıklı bir iletişim dili kullanırım (rahatsız edici söylemler, hakaret veya taciz etmem).	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
12. Benimle ilgili utanç verici bir şey paylaşıldığında (siber zorbalık) veya tehdit içeren bir mesaj aldığımda, saldırgan malzemeyi başkalarına iletmem.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
13. Siber zorbalık içeren bir durumla karşılaştığımda, mümkünse kanıt olması için ekran görüntüsünü alırım.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
14. Çevrimiçi ortamda karşılaştığım saldırgan veya beni rahatsız eden bir durum olduğunda cihazı kapatır ve güvendiğim bir yetişkine (aile, öğretmen, rehber öğretmen) hemen haber veririm.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
15. Çevrimiçi tanımadığım kişilerden gelen mesajlara ve eklenti dosyalarına yanıt vermem veya onları açmam.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Bölüm 4: Çevrimiçi Bilgi ve Öğrenme

Davranış İfadesi	1- Her Zaman	2- Bazen	3- Hiç
16. İnternette gördüğüm bir bilginin (haber, sosyal medya içeriği veya yorum) doğru ve tarafsız olduğundan emin olmak için birden fazla kaynağa başvururum ve eleştirel düşünürüm.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
17. Ödev veya proje yaparken kullandığım kaynakların (resim, metin, video) telif hakkı olup olmadığını kontrol eder ve başkasının çalışmalarını kendi çalışmam gibi göstermemek için kaynak gösteririm.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
18. Çevrimiçi geçirdiğim süreyi, çevrimdışı sosyal, sportif ve okul faaliyetleriyle dengede tutarım.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
19. Çevrimiçi tanıştığım ve gerçekte hiç görmediğim biriyle yüz yüze buluşmaya karar vermeden önce mutlaka bir yetişkine söylerim ve izin alırım.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
20. Çevrimiçi ortamda kendi gelişimim için faydalı olabilecek (eğitim, yabancı dil, kodlama) içerikleri bulmaya çalışırım.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Değerlendirme Sonuçları ve Yönlendirme

Toplam Puan Hesaplaması: (Her Zaman = 3, Bazen = 2, Hiç = 1)

Toplam Puan: / 60

Sonuçların Yorumlanması (Referans:)

Puan Aralığı	Değerlendirme	Geliştirme Alanları
50 - 60 Puan:	Tebrikler! Dijital dünyada dikkatli, güvenli ve sorumlu bir kullanıcı (Dijital Vatandaş) olma konusunda güçlü bir bilince sahipsiniz.	Davranışlarınızı sürdürün ve çevrenizdeki kişilere rol model olun.
38 - 49 Puan:	Geliştirilebilir Alanlar Var. Siber zorbalığa maruz kalma riskiniz olabilir veya mahremiyetinizi koruma konusunda bazı eksikleriniz bulunuyor. Daha dikkatli olmanız gerekiyor.	Özellikle Bölüm 1 ve 2'deki "Bazen" yanıtlarınızı gözden geçirin ve güvenlik önlemlerini artırın.
37 Puan ve Altı:	Ciddi Riskler. Kişisel verileriniz tehlikede olabilir ve dijital dünyanın zorluklarıyla başa çıkmakta zorlanabilirsiniz.	Bu formu aileniz ve öğretmeninizle birlikte inceleyin. Bölüm 3'teki " Hiç " yanıtlarınızı (yardım isteme, zorbalık sergilememe) mutlaka düzeltmelisiniz.

Öğrenci Yorumu/Taahhüdü: *Bu değerlendirme sonucunda, çevrimiçi davranışlarımda özellikle hangi alanlara daha fazla dikkat edeceğimi buraya not ediyorum.*

[Öğrencinin kendi taahhüdü buraya yazılacaktır. Örnek: "Şifrelerimi daha güçlü yapmaya ve yabancıardan gelen mesajlara yanıt vermemeye dikkat edeceğim."]