KÜTAHYA ORGENERAL ASIM GÜNDÜZ İLKOKULU E-GÜVENLİK PLANI

Günümüz dünyasında çocuklar ve teknoloji çoğu zaman birbirinden ayrılamaz. Web'in kullanımı artıyor olsa da, güvenli kullanımı sorunu da artıyor. Güvenli bir ortam sağlamak için, risklerin türlerini ve sıklıklarını ve bunları azaltacak ve hatta daha iyi ortadan kaldıracak çözümleri anlamalıyız. Çocukların çevrimiçi ortamda karşılaştıkları riskleri ele alan, daha genç kullanıcılar için daha güvenli bir internet oluşturmanın yolları üzerine pek çok araştırma yapılmıştır.

Çocukların çevrimiçi ortamda karşılaştıkları risklerden biri siber zorbalık veya çevrimiçi mağduriyet, yani elektronik iletişim araçları aracılığıyla zorbalık veya tacizdir. Bazı siber zorbalık örnekleri açıkça tanınabilirken, diğerleri daha az tanınabilir. Siber küfürlü dilin ve korkutma taktiklerinin açıkça bir suça işaret ettiği durumlar olabilir ve bazı durumlarda bu sadece bir kişinin kötü davranışıdır. ve bu onun yaygınlık istatistiklerini etkiler. Çevrimiçi siber zorbalıkla mücadele etmenin bir yolu, okul zorbalığı ile siber zorbalık arasındaki bağlantıyı kullanmaktır. Çocukların ilişkilerini ve tutumlarını geliştirmeye yönelik girişimlere okul zorbalığı denir. Siber zorbalıkla mücadelede potansiyel olarak etkili önleyici tedbirler olarak kabul edilirler ve siber zorbalıkla mücadelede de faydalı olabilirler. Gençler ve yetişkinler genellikle internet kurbanı olma konusunda farklı yorumlara sahiptir. Yetişkinler belirli etkinliklerle belirli bir şekilde ilişki kurma eğilimindedir, ancak gençler aynı örnekleri akranları arasındaki ortak etkinlikler olarak tanımlayabilir, ancak çevrimdışı bir sorunla başlarlar. Okullar, okul çapında zorbalık önleme programının oluşturulmasını kolaylaştırmak için politikalar geliştirir ve bu programlar genellikle etkinliklerinin düzenli olarak değerlendirilmesini içerir. Başarılı ve etkili programlar, bireysel öğrencilerden ve sınıflardan öğretmenlere ve öğrenci zorbalıkla mücadele ekiplerine kadar okulun her seviyesinde zorbalıkla mücadele stratejilerini teşvik eder. Ağır web kullanıcıları uygunsuz içerikle karşılaşabilir. Gençler genellikle çevrimiçi olarak cinsel tacize veya cinsel içeriğe maruz kalabilir. Çevrimiçi sınırsız içerik, olgunlaşmamış gençleri büyük miktarda istenmeyen cinsel içerik ve bilgiye maruz bırakabilir. Örnekler arasında cinsel istekler, cinsel konuşmalar, cinsel fotoğraflar gönderme veya talep etme veya istenmeyen cinsel bilgiler yayınlama yer alır. Ayrıca, gençler istenmeyen pop-up'lar aracılığıyla çevrimiçi olarak cinsel olmayan içerik aradıklarında, bazen uygunsuz içerik veya cinsel resimler/videolar bulurlar. E-posta dolandırıcılığı alabilirler. İstenmeyen cinsel karşılaşmalarla baş etmenin en yaygın yolu, gençleri bu tür hizmet sağlayıcıları engellemeye teşvik etmek veya onlara yardım etmek ya da sorun yaşadıkları çevrimiçi forumu terk etmektir. Çünkü çoğu genç, kafa karışıklığı nedeniyle çevrimiçi olarak tanıştıklarında yetişkinleri dahil etmez. , ebeveynler ve öğretmenler gençlerin mücadele ettiğine inanıyor. Bu nedenle okullar veya belediyeler genellikle kurslar ve bilgilendirici tartışmalar düzenlerken, diğer etkili yöntemler arasında filtreleme ve güvenlik duvarı teknolojileri yer alır. Ek olarak, İnternet erişim şirketleri, kullanıcılara daha güvenli çevrimiçi ortamlar sağlayarak, çevrimiçi risklerle başa çıkmanın başka bir yolunu teşvik eder. Gençler çevrim içi mahremiyetlerini koruma konusunda daha aktif olursa, İnternet'in ortaya koyduğu risklerin çoğu azaltılabilir. Kişisel bilgileri çevrim içi olarak ifşa etmeye daha az istekli olmaları ve mahremiyetlerini nasıl yöneteceklerini bilmeleri için eğitilmeleri gerekir. Bu tür eğitim özellikle küçük yaşlardan itibaren okullarda önemlidir. Ebeveynler ve çocuklar arasındaki nesil farkı nedeniyle, birbirlerine olan güvenlerini engelleyebilecek ve böylece çevrimiçi risklerin etkili bir şekilde azaltılmasına yol açabilecek yanlış anlamalar ortaya çıkabilir. , gençler ve yetişkinler arasındaki iletişim teşvik edilmelidir Siber güvenlik hakkında bir diyalog başlatmak, açığı kapatmaya ve güvenlik önlemlerini iyileştirmeye yardımcı olabilir. yarın dünya liderleri arasında. İnternetin faydaları modern kültürümüzün bir parçasıdır ve birçok teknolojik gelişmemizin gençlerin güvenliğine yansımasına izin vermemeliyiz.

E GÜVENLİK MÜFREDATIMIZ HAKKINDA

• Derslerde internet kullanımına ilişkin içerikler modern ve teknolojik gelişmelere göre modernize edilmiştir. • İnternetin bilinçli ve güvenli kullanımı konusunda bilgi, beceri ve tutum geliştirmeye yönelik seminerler düzenlenmektedir. Okulun BİT koordinatörü öğretmen, müfredatta internetin, özellikle sosyal medyanın bilinçli kullanımı ile ilgili konularda güncel bilgiler aldı. • BTK, Fatih projesinin uygulama ve bakımında teknolojinin etkin ve güvenli kullanımını sağlamak için güvenli bir internet ağı kullanmaktadır. • MEB okullarında elektromanyetik kirlilik ve internet güvenliği önemlidir.

ÇOCUKLARA YÖNELİK e GÜVENLİK ÖNLEMLERİ

• Çocuklar ve gençler için rehberli, sınırlı ve aile erişimi sağlayabilecekleri bilincini uygularız. • Hükümet politikası, İnternet'in güvenli kullanımıyla ilgili paketleri teşvik etmek ve dağıtmaktır. • Evde sınırlı internet paketlerinin kullanılması tavsiye edilir. • Kullanıcı farkındalığına yönelik uygulamalar geliştirmek için derslerde bu konuya öncelik verilir. •Aileleri kontrol yöntemleri ve teknolojik olanaklar konusunda bilinçlendirmek, gerekli uygulamaları geliştirmek ve yaygınlaştırmak. Üniversite araştırmacıları tarafından yardım isteniyor.

CEP TELEFONU KULLANIMI

1. Öğretmenlerin ve destek personelinin, öğrencilerin bulunduğu yerde ve zamanda cep telefonlarını kullanmalarına izin verilmez.

2. Öğrenciler otobüsle gelip gittikleri ve otobüsle öğrenciye ulaşım kolay olduğu için okula gelirken cep telefonu getiremezler. Herhangi bir nedenle okula cep telefonu getirmesi gereken öğrenciler, cep telefonunu açılmamış olarak okul idaresinin belirleyeceği bir yere ve okul çıkışı görevliye teslim etmek zorundadır. Öğrencinin sınıfta cep telefonu bulundurması ve dolayısıyla kullanması yasaktır.

3. sınıfta ve okul binasında cep telefonu bulundurma yasağını ihlal eden öğrencinin cep telefonu okul idaresine bir hafta süreyle (süre sonunda iade edilmek üzere) el konulur. birinci suç için iki hafta ve üçüncü suç için tam süre. Kural ihlali durumunda öğrenci velisinin bu etki aracını destekleyebilmesi için velinin akademik yılın başında (veya öğrenci kayıtlı) elde edilir. . .

4.Okul içindeki wifi bağlantısını hiçbir öğrenci kullanamaz. Yani öğrencinin herhangi bir şekilde şifreyi ele geçirmesi ve kablosuz ağa bağlanması yasaktır. Bu yasağa uymayan öğrencinin cep telefonuna bir hafta süreyle el konulur.

5. Okul ve sınıf sınırları içinde, ders etkinlikleri sırasında, öğretmen gözetiminde ve sadece acil durumlarda öğrenci cep telefonunu kullanabilir. Bunun dışındaki amaçlar için kullanılmasına izin verilmez.

6. Öğrencinin cep telefonu numarası, öğrencinin velisinin izni dışında kimse tarafından bilinemez.

7. Her yıl eğitim-öğretim yılının başında velilerle cep telefonu kullanımının tartışıldığı toplantılar düzenlenir.

8. Yılda üç kez yapılan öğretmenler genel kurulunda (dersin başında, ortasında ve sonunda) öğretmenlerle okulun güvenliğini ve dolayısıyla cep telefonu politikasını tartışıyoruz. Ülkenizde yasal olup olmadığına bakılmaksızın, okulunuzun net bir fotoğraf ve görüntü politikası olduğundan emin olun.

OKULUMUZDA FOTOĞRAF YA DA VİDEO ÇEKİMİ VE YAYINLANMASI

1. Öğrenci velilerinin isteği üzerine, okul içinde ve okul bahçesi içinde, okul yönetiminin belirleyeceği kişiler dışında, etkinlik ve program saatleri dışında fotoğraf ve video çekilemez. Bu yasak, bir öğrencinin başka bir öğrencinin fotoğrafını çekmek veya videoya çekmek istemesi durumunda da geçerlidir.

2. Okul idaresinin görevlendireceği kişiler tarafından çekilen resim ve videolar, ancak velisinin talebi ve yazılı izni ile eğitim kurumunun resmi internet sitesinde ve sanal ortamlarda yayınlanabilir. Velisi öğrenciye izin vermeyen öğrencinin fotoğraf ve videoları yayınlanmayacaktır.

3. Velilerin fotoğraf ve videolarının çekilip yayınlanmasına izin vermemesi durumunda, fotoğraf çekimi sırasında öğrenciler üzerinde psikolojik baskı oluşmaması için önlemler alınır. . Okul yetkilileri tarafından yayınlanan resim ve videolara öğrencilerin kişisel bilgileri kesinlikle eklenmeyecektir. Öğrenciler, bir video konferans araması veya mesajı hazırlamadan veya yanıtlamadan önce eğitmenlerinden izin ister. Video konferans, öğrencilerin yaş ve yeteneklerine göre yönlendirilir. (okullar bunun nasıl uygulanacağını ve gerçekleştirileceğini listelemelidir) Çocuklar video konferans faaliyetlerine katılmadan önce ebeveynlerden ve velilerden onay alınacaktır. Video konferans, kapsamlı bir risk değerlendirmesinin ardından resmi ve onaylı iletişim kanalları aracılığıyla gerçekleştirilecektir. Video konferans yönetim alanlarına veya uzaktan kontrol sayfalarına yalnızca üst düzey yöneticiler erişebilir. Eğitimli video konferans hizmetleri için benzersiz oturum açma ve parola bilgileri sağlanır ve yalnızca çalışanlara ayrılmıştır.

E-GÜVENLİK POLİTİKAMIZ

Dijital teknolojiler, okul çağındaki çocuklar için de olağanüstü fırsatlar ve imkanlar sunuyor. Çocuklar internet üzerinden kolay ve hızlı bir şekilde bilgi, eğlenceli oyunlar vb. Ancak bu dijital teknolojilerin sunduğu harika olanaklara ek olarak, küçümsenemeyecek bir gerçek daha vardır: çocuğu bekleyen zihinsel, duygusal ve fiziksel saldırılar ve tuzaklar. Örneğin, internete maruz kalan bir çocuğun yanlışlıkla bir reklama bakarak pornografik bir siteye ulaşması veya

arama motoruna bilerek veya bilmeyerek girdiği yanlış bir kelime veya bir çocuğun merakını uyandıran görüntü. zihinsel, duygusal ya da fiziksel olarak onu tehdit edebilir, onu çökerten ortamlara neden olabilir. Ebeveynleri korkutan, endişelendiren ve dehşete düşüren çevrimiçi oyunlar tarafından zihinsel veya fiziksel olarak mağdur edilen bir çocuğun haberini duymadığımız gün geçmiyor! Bir çocuğu yukarıda kısaca bahsedilen tehlikelerden korumanın en kesin yolu, onu internet ortamından tamamen uzak tutmaktır. Ne yazık ki hızla gelişen dijital teknolojiler nedeniyle çocuğu online ortamdan tamamen uzak tutmak mümkün olmadığı gibi, tamamen yasaklamak da sorunu çözmemektedir. Ayrıca, çevrimiçi ortamlara erişimin tamamen yasaklanması ve engellenmesi, çevresel faktörler ve ebeveyn tutumları nedeniyle imkansız hale gelmiştir. Bu nedenle çocuğu internet ortamının tehlikelerinden korumak için onu tamamen yasaklamaya çalışmaktan daha etkili yöntemler bulmak gerekmektedir. Öncelikle belirtmek gerekir ki, dijital teknolojilerin sunduğu imkanlar nedeniyle çocuğu söz konusu tehlikelere karşı hiçbir önlem %100 koruyamaz. Dolayısıyla çocuğu bu tehlikelerden korumanın bilgi, farkındalık ve davranış kazanmaktan ve bu amaç doğrultusunda çalışmaktan daha etkili bir yolu yoktur. Bu faktörlerin bir sonucu olarak, okul politikası olarak, öğrencilerimizi çevrimiçi ortamların tehlike ve zararlarından korumak için bilinçli ve bilinçli olarak politikalar uygular, gerekli ve uygulanabilir yasaklar koyarız:

ÇOCUKLARA YÖNELİK E- GÜVENLİK ÖNLEMLERİ

• Çocuklara ve gençlere kontrollü, sınırlı ve uygun kullanımı ailelere sağlamak için eğitim faaliyetleri yürütüyoruz. • Hükümetin politikası internetin güvenli kullanımı ile ilgili paketleri teşvik etmek ve yaygınlaştırmaktır, Telekom bu amaçla güvenli bir internet paketi sunmaktadır. • Evde sınırlı internet paketlerinin kullanılması tavsiye edilir. • Okul ve veliler arasındaki ilişkiler güçlendirilmeli ve teşvik edilmelidir. • Güvenli internet paketlerinin kullanımının yaygınlaşmasına katkıda bulunmalıyız. • Aile bilgisayarları kullanıcıya göre farklı profiller oluşturabilmeli ve bu profillere göre farklı paketlerle korumalı internet hizmeti sunulmalıdır. Bir soruşturma başlatıldı. • Kullanıcı farkındalığına yönelik uygulamalar geliştirmek için derslerde bu konuya öncelik verilir.

OKUL PERSONELİ

Okul personelimiz mesleki gelişim portalı Mehmet GÜNDÜZ e Twinning'in çevrimiçi ve çevrimiçi mesleki gelişim faaliyetlerine katılmıştır. E-Güvenlik Politikası, tüm çalışanların katılması için resmi olarak sunulur ve tartışılır ve kendimizi koruma taahhüdümüzün bir parçası olarak pekiştirilir ve vurgulanır. Çalışanlar, İnternet trafiğinin tek bir kullanıcıya kadar izlenebileceğini ve takip edilebileceğini bilir. Okul sistemlerini ve ekipmanlarını kullanırken dikkat ve profesyonel davranış gereklidir. Hem profesyonel hem de kişisel olarak tüm çalışanlar için düzenli olarak (yılda en az bir kez) güvenli ve sorumlu internet kullanımı konusunda güncel ve ilgili kişisel eğitimler düzenlenmektedir. Tüm personel, çevrimiçi davranışlarının okul içindeki rollerini ve imajlarını etkileyebileceğini bilir. Bir şeyin mesleği veya kurumu güvensiz hale getirdiğine veya kişinin mesleki yeteneklerine olan güvenini kaybetmesine neden olduğuna inanılırsa, kanuni, disiplin veya yasal işlem başlatılabilir. Filtreleme sistemlerini yönetmekten veya bilgi ve iletişim teknolojilerinin kullanımını izlemekten sorumlu çalışanlar, yönetim tarafından denetlenir ve sorunları veya endişeleri bildirmek için açık prosedürlere sahiptir. Okul, personelin öğrencilerin yaşlarına ve yeteneklerine göre kullanması için yararlı çevrimiçi araçlar aramalıdır. Okulun çevrimiçi güvenlik politikasına (e-Güvenlik) ve bültenlerde, mektuplarda, okul broşüründe ve okul web sitesinde ebeveynlerin dikkati çekilir. Evde ve okulda çevrimiçi güvenlik alanında ebeveynlerle işbirliğini teşvik ediyoruz. Bu, evde güvenli internet kullanımı için tanıtım ve öneriler içeren ebeveynler için eğitimi veya diğer geniş katılımlı etkinliklerde internet güvenliğini vurgulamayı içerebilir. veli eğitimleri, toplantılar, spor günleri gibi sosyal etkinlikler düzenlerler. Okul sözleşmesinin bir parçası olarak, ebeveynler internet güvenlik bilgilerini okumalıdır. Ebeveynler, okulun Kabul Edilebilir Kullanım Politikasını okumaya ve çocuklarıyla bunun sonuçlarını tartışmaya teşvik edilir. Ebeveynlere internet güvenliği hakkında çeşitli formatlarda bilgi ve rehberlik sunulmaktadır. Ebeveynler, çocukları için olumlu çevrimiçi davranışı modellemeye teşvik edilir.