



TC
ARTUKLU KAYMAKAMLIĞI
İlçe Milli Eğitim Müdürlüğü
Abdulkadir Tutaşı İlkokulu
e-Güvenlik Okul Eylem Planı

Teknoloji hızla gelişmekte ve internet hayatımızın kaçınılmaz bir parçasıdır. İnternet kullanımı ülkemizde hızla artmakta iken, küçük yaş grubunun bu konu hakkında bilgilendirilmesi gerekmektedir.

E-güvenlik nedir? Aşamaları nelerdir? ve Nelerden kendimizi korumalıyız?

Öğrencilerimizi bu konularda bilinçlendirmeyi amaçlamış bulunmaktayız. Bu eylem planıyla;

- Öğrencilerimizi bilinçli BT araçları ve internet kullanımı hakkında geliştirmek
- Siber zorbalık konusunda bilinçlendirmek
- Siber mağdurluk
- Oltaya gelme
- İnternet etiği
- BT suçları
- Teknolojide üretim konusu
- Avantajlar ve riskler gibi konularda okul paydaşlarını bilgilendirme amaçlanmaktadır.

Çevrimiçi iken çocukların karşılaştığı risklerden biri de siber zorbalık veya çevrimiçi mağduriyettir; yani elektronik iletişim şekillerini kullanan zorbalık veya taciz. Siber zorbalığın bazı örnekleri açıkça tanımlanabilirken diğerleri daha azdır.

Okullar, okul çapında bir zorbalık önleme programının oluşturulmasını kolaylaştıracak politikalar oluşturur ve bu programlar tipik olarak etkinliklerinin periyodik değerlendirmelerini içerir. Başarılı ve etkili programlar, bireysel öğrencilerden ve sınıflardan, eğitimcileri ve öğrencileri birleştiren zorbalık karşıtı takımlara kadar, okulda her seviyede zorbalık karşıtı stratejileri teşvik etmek için çalışır.

Ağır internet kullanıcıları uygunsuz içerikle çevrimiçi karşılaşabilirler. Bunun yanı sıra e-posta dolandırıcılıklarına maruz kalabilirler.

İstenmeyen çevrimiçi iletişimleri engellemenin en uygun yolu, çocukları bu tür sağlayıcıları engellemeye teşvik etmek veya onlara yardım etmek veya sorun yaşadıkları çevrimiçi forumdan ayrılmalarını sağlamaktır. Bazı çocuklar, utanç yüzünden çevrimiçi olarak karşılaştıkları uygunsuz durumlara yetişkinleri dâhil etmeme eğiliminde oldukları için, ebeveynlerin ve eğitimcilerin, gençlerin zorluklarla karşılaşabileceğini belirtmek için dikkat etmeleri gereken işaretlerden haberdar edilmesi gerekir. Bu nedenle, kurslar ve bilgilendirici görüşmeler genellikle okullarda veya yerel konseyler tarafından organize edilirken, diğer etkin yöntemler filtreleme ve güvenlik duvarı teknolojilerini içerir. Buna ek olarak, internet erişimi sağlayan şirketlerin kullanıcıları için daha güvenli çevrimiçi ortamlar sağlamaları, dolayısıyla çevrimiçi riskleri ele almanın bir başka yolunu teşvik etmeleri önerilmektedir.

Çocukların çevrimiçi mahremiyetlerini korumaları durumunda, internetin oluşturduğu risklerin birçoğu azaltılabilir. Kişisel bilgilerin çevrimiçi olarak açığa çıkmasına daha az istekli olacak şekilde eğitilmeleri ve gizliliklerini nasıl yöneteceklerini bilmeleri gerekir; Bu tür eğitim, özellikle küçüklükten itibaren okullarda verilmesi önemlidir.

E-GÜVENLİK POLİTİKAMIZ

Dijital teknolojiler okul çağı çocukları için de olağanüstü imkânlar ve fırsatlar sunuyor. Çocuklar da internet ortamının sağladıkları bilgiye, eğlenceli oyunlara ve benzeri etkinliklere kolayca ve



hızlıca erişim sağlayabiliyorlar. Ancak, dijital teknolojilerin sağladığı bu harika imkanların yanında, çocuğun zihinsel, ruhsal ve fiziksel saldırılarla, tuzaklarla karşılaşması tehlikesinin varlığı da hafife alınamaz bir gerçekliktir. Örnek vermek gerekirse internet ortamındaki bir çocuğun istem dışı da olsa karşısına çıkan bir reklamı izleme yoluyla ya da arama motoruna bilerek-bilmeyerek yazacağı yanlış bir kelime sebebiyle pornografik bir siteye girmesi mümkündür ya da çocuğun merakını kışkırtan bir görsel onu zihinsel, duygusal ya da fiziksel olarak tehlikeye düşürecek ortamlara sürükleyebilir. Gün geçmiyor ki, bazı çevrimiçi oyunlar sebebiyle ebeveynleri korkutan, endişeye ve dehşete düşüren, ruhsal ya da fiziksel olarak mağdur olmuş bir çocukla ilgili bir haber duymamış olalım!

Yukarıda kısaca söz edilmiş olan tehlikelerden çocuğu korumanın en emin yolu, onu internet ortamından tamamen uzak tutmaktır. Ancak çok hızlı gelişen dijital teknolojiler sebebiyle ve ne yazık ki, çocuğu internet ortamından tamamen uzak tutmak mümkün olmamakta, tamamen yasaklamak sorunu çözmemektedir. Kaldı ki çevresel etkenler ve ebeveyn tutumları sebebiyle internet ortamlarını tamamen yasaklamak ve erişimi engellemek imkânsız bir hal almıştır. Bu sebeple çocuğu internet ortamının oluşturduğu tehlikelerden korumak için tamamen yasaklamaya çalışmaktan daha etkili tedbirler bulmak zorunluluğu vardır.

Öncelikle ifade etmek gerekir ki, dijital teknolojilerin sahip olduğu imkanlar sebebiyle alınabilecek hiçbir tedbir çocuğu yukarıda sözü edilen tehlikelerden yüzde yüz oranında koruyamayacaktır. Dolayısıyla söz konusu tehlikelerden kendisini koruması için çocuğa bilgi, bilinç ve davranış kazandırmaktan, bu hedef için çaba harcamaktan daha etkili bir yol kalmamaktadır.

Bu gerçekler sebebiyle, okul politikası olarak öğrencilerimizi internet ortamlarının tehlikelerinden ve zararlarından koruyabilmek için ısrarlı ve kararlı bir şekilde uygulamalar gerçekleştirerek, gerekli ve uygulanabilir planlamalar yapmaktayız.

E GÜVENLİK MÜFREDATIMIZ HAKKINDA

- Çocuklarda bilinçli ve güvenli internet kullanımına dair bilgi, beceri ve tutumların geliştirilmesi için seminerler düzenlenmektedir.
- Türkçe, Fen Bilimleri, Hayat Bilgisi , Rehberlik ve Serbest Etkinlik saatlerinde “Siber Mağdurluk ve İnternet Kullanımı” gibi konuların işlenmesi sağlanmaktadır.
- Fatih projesinin yürütülmesi ve sürdürülmesi aşamasında teknolojinin etkili ve güvenli kullanımlarının sağlanması için BTK tarafından güvenli internet ağı mevcuttur.
- MEB'e bağlı okullarda elektromanyetik kirliliğe ve internet güvenliğine önem verilmektedir.

ÇOCUKLARA YÖNELİK e-GÜVENLİK ÖNLEMLERİ

- Aileye yönelik çocuk ve ergenlere denetimli, sınırlı ve amaçlı kullanım sağlayabilmeleri ile ilgili bilinçlendirme çalışmaları yapmaktayız.
- İnternetin güvenli kullanımı ile ilgili paketlerin tanıtım ve yaygınlaşmasını sağlamak devlet politikasıdır.
- Evlerde limitli internet paketlerinin kullanımını teşvik etmek için sınıf rehber öğretmenlerimiz tarafından rehberlik yapılmaktadır.
- Kullanım farkındalığına yönelik uygulamalar geliştirmek için derslerde bu konuya öncelik verilmektedir.
- Ebeveynleri denetim yolları ve teknolojik imkânları ile ilgili bilinçlendirmek ve gerekli uygulamaları geliştirmek ve yaygınlaştırmak için toplantılarla, sınıf rehber öğretmenleri tarafından planlanan sunum ve bilgilendirme seminerleriyle gerekli destek sağlanmaktadır.
- Okulumuz rehber öğretmeni tarafından öğrencilerimize Teknoloji Bağımlılığı Ve Güvenli İnternet seminerleri yapılmaktadır.



CEP TELEFONU ve AKILLI SAAT KULLANIMI

1. Öğretmenler ve yardımcı hizmetler personeli cep telefonlarını öğrencilerin bulunduğu zaman ve ortamlarda (Ders ve Etkinlik Saatlerinde) kullanamazlar.
2. Okulumuz ilkökul kademesi olduğu için cep telefonu kullanımı yoktur. Ancak akıllı saat kullanımı söz konusudur. Herhangi bir öğrencinin akıllı saatini ders esnasında kullanmasına izin verilmemektedir.
3. Öğrenci cep telefon (akıllı saat içinde bulunan hat) numarasının, öğrenci velisinin izin verdiği kişiler dışındakiler tarafından öğrenilmesine izin verilmez.
4. Velilerle her yıl, eğitim öğretim yılı başında akıllı saatlerin kullanımı konusunda bilgi verme amaçlı sınıf öğretmenleri tarafından toplantılar yapılır.
5. Öğretmenlerle (eğitim öğretim başında, ortasında ve sonunda olmak üzere) yılda üç kez yapılan öğretmenler genel kurulunda okul güvenliği ve dolayısıyla akıllı saat kullanımı politikası hakkında değerlendirme amaçlı tartışmalar yapılır.

OKULUMUZDA FOTOĞRAF YA DA VİDEO ÇEKİMİ VE YAYINLANMASI

1. Okul idaresi tarafından görevli kılınanlar haricindeki kişiler tarafından ve öğrenci velilerinin bilmek istedikleri etkinlik ve programlar dışındaki zamanlarda, okul ve okul bahçesi sınırları içerisinde fotoğraf ve video çekimi yapılamaz. Bu yasak bir öğrencinin diğer bir öğrencinin fotoğraf ve videosunu çekmek istemesi durumunda da geçerlidir.
2. Okul idaresi tarafından görevlendirilen kişilerin çektiği fotoğraf ve videolar ancak Okulun resmi web adresinde ve sanal ortamlarında, ilgili öğrenci velisinin talep ve yazılı onayı ile yayınlanabilir. Öğrencisi için onay vermeyen velinin öğrencisi ile ilgili fotoğraf ve videolar yayınlanmaz.
3. Velisi tarafından fotoğraf ve video görüntülerinin çekilip yayınlanmasına onay verilmeyen öğrencilerin, çekim esnasında psikolojik baskı yaşamaması için tedbirler alınır.
4. Okul görevlileri tarafından yayınlanan resim ve videolarda öğrencilerin kişisel bilgilerine kesinlikle yer verilmez. Öğrenciler, bir video konferans araması veya mesajı hazırlamadan veya cevaplamadan önce bir öğretmeninden izin isteyecektir. Video konferans, öğrencilerin yaşı ve yeteneği için uygun bir şekilde denetlenecek. (okullar bunun nasıl uygulanacağını ve başarılacağını listelemelidir) Veliler ve bakıcıların rızası, çocuklar video konferans faaliyetine katılmadan önce alınacaktır. Video konferans, sağlam bir risk değerlendirmesini takiben, resmi ve onaylanmış iletişim kanalları vasıtasıyla gerçekleşecektir. Sadece ana yöneticilere video konferans yönetim alanlarına veya uzaktan kumanda sayfalarına erişim hakkı verilmektedir. Eğitimli video konferans servisleri için benzersiz oturum açma ve şifre bilgileri yalnızca personel üyelerine verilecek ve güvence altına alınmış olacaktır.

OKUL PERSONELİ

Okulumuzda mesleki gelişim portallarından çevrimiçi mesleki gelişim etkinliklerine katılan öğretmenlerimiz bulunmaktadır. Hedeflerimizden birisi de çevrimiçi güvenlik (e-Güvenlik) politikası, tüm çalışanların katılımı için resmi olarak sağlanması ve korunma sorumluluğumuzun bir parçası olarak güçlendirilmesi ve vurgulanmasıdır. Personel, İnternet trafiğinin izlenebileceğini ve tek bir kullanıcıya kadar izlenebileceğinin farkında olacaktır. Okul sistemlerini ve cihazlarını kullanırken takdir yetkisi ve profesyonel davranış gereklidir. Personelin tüm üyelerine, profesyonel ve kişisel olarak, güvenli ve sorumlu İnternet kullanımı konusunda güncel ve uygun personel eğitimi, düzenli (en az yıllık) temelde çeşitli şekillerde sağlanacaktır. Çalışanların hepsi, çevrimiçi davranışlarının okuldaki rolü ve itibarını etkileyebileceğinin farkına varacaktır. Mesleği veya kurumu tehlikeli duruma düşürdüğü veya mesleki yeteneklerine güvenini kaybetmiş bir şeyin bulunduğu düşünülürse, disiplin veya hukuki önlemler alınabilir. Filtreleme sistemlerini yönetme veya BİT kullanımını izleme sorumluluğu taşıyan personelin



üyeleri, okul idaresi tarafından denetlenecek ve sorunları veya endişeleri bildirmek için açık prosedürlere sahip olacaklardır.

Okul çalışanları, öğrencilerin yaşlarına ve yeteneklerine göre kullanması gereken yararlı çevrimiçi araçları kontrol etmelidir. Çocukların, internetin ve dijital teknolojinin güvenilir ve sorumlu kullanıcıları olabilmesi için ana-babanın / bakıcıların oynayacakları önemli bir role sahip olduklarını kabul etmelidirler. Ebeveynlerin dikkatleri, bültenler, mektuplar ve okul web sitesinde okulun çevrimiçi güvenlik (e-Güvenlik) politikasına ve beklentilerine yönelecektir.

Evde ve okulda ebeveynlerle çevrimiçi güvenlik konusundaki işbirlikçi, yaklaşımı teşvik edilecektir. Okul Anlaşması'nın bir parçası olarak ebeveynlerin çevrimiçi güvenlik bilgilerini okumaları istenecektir. Ebeveynler, Okula Kabul Edilebilir Kullanım Politikası'nı okumaya ve çocuklarıyla etkilerini tartışmaya teşvik edilecektir. Çevrimiçi güvenlik konusundaki ebeveynler için bilgi ve rehberlik, ebeveynlere çeşitli biçimlerde sunulacaktır.

Okulumuzun e-Güvenlik politikasının belirlenmesi, eğitimlerin verilmesi ve çalışma planının hazırlanmasında aşağıdaki web adreslerinden faydalanılmıştır.

Kaynakça:

- "Daha Güvenli İnternet Merkezi (gim.org.tr)
- Safer Internet Center'ın resmi sayfası (https://ec.europa.eu/info/index_en)
- Güvenli Web (guvenliweb.org.tr) - çevrimiçi güvenlik konuları için farkındalık portalı.
- Güvenli Çocuk (guvenlicocuk.org.tr) - 13 yaşından küçük çocuklar için oyun ve eğlence portalı.
- İhbar Web (ihbarweb.org.tr) - yasadışı içerik için telefon hattı.
- İnternet BTK (internet.btk.gov.tr) - İnternet ve BT yasası konusunda farkındalık portalı."

