İMKB ÖZEL EĞİTİM UYGULAMA OKULU (I.II. III. KADEME)

E-GÜVENLİK POLİTİKAMIZ

Digital teknolojiler okul çağı çocukları için de olağanüstü imkânlar ve fırsatlar sunuyor. Çocuklar da internet ortamının sağladıklarıyla bilgiye, eğlenceli oyunlara ve benzeri etkinliklere kolayca ve hızlıca erişim sağlayabiliyorlar. Ancak, digital teknolojilerin sağladığı bu harika imkânların 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 online oyunlar sebebiyle ebeveynleri korkutan, endişeye ve dehşete düşüren, ruhsal ya da fiziksel olarak mağdur olmuş bir çocukla ilgili bir haber duymamış olalım!

Çok hızlı gelişen digital teknolojiler sebebiyle 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, digital teknolojilerin sahip olduğu imkânlar sebebiyle alınabilecek hiç tedbir çocuğu yukarıda sözü edilen tehlikelerden yüzde yüz oranında koruyamayacaktır. Dolayısıyla söz konusu tehlikelerden kendisini koruması için çocuğa bilgi ve davranış kazandırmaktan, bu hedef için çaba harcamaktan daha etkili bir yolumuz yoktur.

Bu gerçekler sebebiyle, okul politikası olarak öğrencilerimizi internet ortamlarının tehlikelerinden ve zararlarından koruyabilmek için ısrarlı ve kararlı bir şekilde uygulamalar gerçekleştirecektir.

İnternet toplu kullanım sağlayıcılarının yükümlülükleri

MADDE 4 – (1) İnternet toplu kullanım sağlayıcılarının yükümlülükleri şunlardır:

a) Konusu suç oluşturan içeriklere erişimi önleyici tedbirleri almak amacıyla içerik filtreleme sistemini kullanmak.

İnternet ortamı insanların gerçek hayatta olduğu gibi kendilerini diledikleri gibi ifade edebilecekleri, istedikleri bilgiye istedikleri anda ulaşabilecekleri özgür bir alandır. İnsanlar iletişim özgürlüğüne sahip olduğu gibi erişim özgürlüğüne de sahiptirler ve bu anayasamızda güvence altına alınmıştır. Bu alanı kullanırken aynen gerçek hayatta olduğu gibi birtakım kişilik haklarına riayet edilmesi ve çevrimiçi ortamın bu hak ve sorumluluklara göre kullanılması için birtakım hukuki düzenlemeler yapılmıştır.

Çevrimiçi ortamda var olan bazı bilişim suçları şunlardır:

1. Bilgisayar Sistemlerine ve Servislerine Yetkisiz Erişim
2. Bilgisayar Sabotajı
3. Bilgisayar Yoluyla Dolandırıcılık
4. Bilgisayar Yoluyla Sahtecilik
5. Bir Bilgisayar Yazılımının İzinsiz Kullanımı
6. Kişisel Verilerin Kötüye Kullanılması
7. Sahte Kişilik Oluşturma ve Kişilik Taklidi
8. Yasadışı Yayınlar
9. Ticari Sırların Çalınması
10. Terörist Faaliyetler
11. Çocuk Pornografisi
12. Hacking
13. Diğer Suçlar (Organ, fuhuş, tehdit, uyuşturucu, vb.)

Türk Ceza Kanunu'nun 243, 244 ve 245. maddeleri bilişim vasıtasıyla işlenen suçlara düzenleme getirmiştir. 243. madde ile bir bilişim sisteminin bütününe ve bir kısmına hukuka aykırı, olarak girilmesi ve orada kalmaya devam edilmesi suç olarak düzenlenmiştir. 244. madde ile bir bilişim sisteminin işleyişini engelleyen veya bozan bir kişi bir yıldan beş yıla kadar hapis cezası ile cezalandırılır hükmü ile bir bilişim sistemindeki verileri bozan, yok eden, değiştiren veya erişilmez kılan, sisteme veri yerleştiren var olan verileri başka bir yere gönderen kişi altı aydan üç yıla kadar hapis cezası ile cezalandırılır hükmü getirilmiştir. 245. madde ile de banka ve kredi kartlarının kötüye kullanılması eylemleri bağımsız bir suç tipi olarak düzenlenmiştir. Kredi kartı veya banka kartıyla gerçekleştirilen her türkü hukuka aykırı yarar sağlama eylemi bu suç tipini oluşturmaktadır.

Bilişim suçları yanı sıra internet içerik düzememelerine birden fazla kanunda yer verilmekle birlikte bunlardan en önemlisi olan 5651 sayılı "İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun" 2007 yılında yürürlüğe girmiştir. Kanun ile ilk defa internet ortamındaki katalog suçlar kapsamındaki yasadışı içerik ile ilgili erişimin engellenmesi usul ve esasları düzenlenmiş ve internet hizmeti veren internet aktörlerine de bir takım yükümlülük ve sorumluluklar getirilmiştir. Kanunda tanımlanmış katalog suçlara ilişkin; Bilgi Teknolojileri ve İletişim Kurumu Bilgi ve İhbar Merkezi; vatandaşların bu suçlara ilişkin şikâyetlerini bildirebilecekleri müracaat merkezi olarak kurulmuştur. 23.11.2007 tarihinde faaliyete geçen bu merkeze http://www.ihbarweb.org.tr adlı web adresinden yasadışı içeriğe ilişkin ihbarda bulunabilmektedir. Kanun kapsamında ayrıca vatandaşlara internet ortamında kişilik haklarının ihlali ve özel hayatın gizliliği ile ilgili olarak başvuru süreçleri tanımlanmıştır.

6698 Sayılı Kanun-Kişisel Verilerin Korunması Kanunu

Madde 5:Kişisel Veriler ilgili kişinin açık rızası olmaksızın işlenemez.

Madde 8: Kişisel Veriler ilgili kişinin açık rızası olmaksızın aktarılamaz.

Kurum olarak güvenliğimiz çerçevesinde Öğrencilerimizi zararlı bilgi ve kaynaklardan korumakla yükümlüyüz. Yüklenen ve kullanılan programların kullanıcı sözleşmelerini sonuna kadar okumaya özen göstermekteyiz.

Okulda cep telefonu kullanımı hakkında ilgili yönetmelik maddeleri aşağıdadır. Yönetmelik maddelerinde geçen Bilişim Araçları sözcüğünün ne anlama geldiği aşağıda açıklanmıştır.

"Bilişim araçları: Ses ve görüntü kaydı yapma özelliği olan cep telefonu ve kamera ile bilgi toplama, saklama, tasarlama, işleme, aktarma ve çoğaltmada kullanılan bilgisayar, internet , MP3 çalar, DVD, CD, çağrı cihazı ve benzeri araçları ifade etmektedir.

1) OKUL-AİLE MUTABAKATI: Öncelikle okulumuza öğrenci kabulü esnasında velilerimiz ile e-güvenlik konusunda tam bir anlayış birliği sağlarız. Bu anlayış birliği, çocuğun kontrolsüz şekilde internete girmesini ve bilgisayar oyunlarına katılmasını engellemeyi kabul etme gerekliliği ile başlar. Diğer bir ifadeyle, aile ve okul olarak, çocuğun kontrolsüz bir şekilde internet ortamlarında bulunmasına göz yummanın çocuğu geliştirmek ya da özgür bırakmak değil, bağımlılık oluşturucu etkisi sebebiyle çocuğun iradesini ortadan kaldıran ve dolayısıyla özgürlüğünü elinden alan bir potansiyel tehlike olarak değerlendirir ve tedbirler alınması ve uygun çalışmalar yapılması konusunda mutabakat sağlarız.

2) VELİ SEMİNERLERİ: Öğrenci velilerine yönelik olarak zaman zaman tekrar eden e-güvenlik seminerleri ve sunumları gerçekleştirmek suretiyle sürekli olarak değişen ve gelişen digital teknolojilerin oluşturduğu tehlikeler konusunda öğretmen ve velilerin bilgi ve bilinçlerini güncel ve canlı tutarız.

3)ETKİN VE YAKIN TAKİP: Öğrenciyi okulda ve etkin bir şekilde takip ve kontrol ederek, internetin oluşturduğu tehlikelere karşı sürekli güncellenen tedbirler geliştiririz. Okul ve aile işbirliği ile çocuğun gizli-saklı değil, alenî ve kontrollü bir şekilde internete girmesini ve digital teknolojilerden yararlanmasını sağlarız.

4) ÖĞRENCİYE OTOKONTROL BİLİNCİ KAZANDIRMAK: Diğer yandan çocuğu etkili bir şekilde takip ve kontrol ederken, bu takip ve kontrollerin çocuğun yararına olduğu için yapıldığı çocuğa doğru ve ikna edici bir şekilde anlatır ve onun rızasını elde etmeye çalışırız. Bu çaba aynı zamanda çocuğa oto kontrol anlayışı ve davranışı kazandırmayı da hedeflemektedir. İnternet ortamlarının bünyesinde barınan ve çocuğun istismarını hedefleyen tehlike ve tuzaklardan, online oyunların oluşturduğu tehlike ve zararlardan neden korunması gerektiği bilincini öğrenciye kazandırmak en önemli hedefimizdir.

5) DİGİTAL TEKNOLOJİLERİN OLUŞTURDUĞU TEHLİKELERDEN NASIL KORUNACAĞININ ÖĞRENCİYE ÖĞRETİLMESİ:

Digital teknolojilerin tehlikelerinden nasıl korunacağını öğrenciye öğretmek, öğrenci velileriyle bu konuda tam bir işbirliği yapmak öncelikli uygulamalarımız arasındadır.

Amaçlar ve politika kapsamı

• Selçuklu Öğretmen Fatma Menekşe Özel Eğitim Uygulama Okulu, çevrimiçi güvenliğin (e-Güvenlik), bilgisayarlar, tabletler, cep telefonları veya oyun konsolları gibi teknolojiyi kullanırken, dijital dünyadaki çocukların ve yetişkinlerin korunması için vazgeçilmez bir unsur olduğuna inanmaktadır.

• Selçuklu Öğretmen Fatma Menekşe Özel Eğitim Uygulama Okulu, internetin ve bilgi iletişim teknolojilerinin günlük yaşamın önemli bir parçası olduğuna inanır. Dolayısıyla, riskleri yönetmeleri ve bunlara tepki vermek için stratejiler geliştirmenin yollarını öğrenmeleri için çocuklar desteklenmelidir.

• Selçuklu Öğretmen Fatma Menekşe Özel Eğitim Uygulama Okulu, Eğitim standartlarını yükseltmek, başarıyı teşvik etmek, personelin mesleki çalışmalarını desteklemek ve yönetim işlevlerini geliştirmek için toplumun kaliteli İnternet erişimi sunma yükümlülüğüne sahiptir.

• Selçuklu Öğretmen Fatma Menekşe Özel Eğitim Uygulama Okulu, tüm çocukların ve personelin çevrimiçi olarak potansiyel zararlardan korunmasını sağlamakla sorumludur.

• Bu politika, yöneticiler, öğretmenler, destek personeli, çocuklar ve ebeveynler için hazırlanmıştır.

• Bu politika, internet erişimi ve kişisel cihazlar da dahil olmak üzere bilgi iletişim cihazlarının kullanımı için geçerlidir; çocuklar, personel ya da diğer kişilere, çalıştıkları dizüstü bilgisayarlar, tabletler veya mobil cihazlar gibi uzaktan kullanım için okul tarafından verilen cihazlar için de geçerlidir. Tüm çalışanların sorumlulukları şunlardır:

• Çevrimiçi güvenlik politikalarının geliştirilmesine katkıda bulunmak.

• Kabul Edilebilir Kullanım Politikalarını okumak ve onlara bağlı kalmak.

• Okul sistemlerinin ve verilerin güvenliğinden sorumlu olmak.

• Bir dizi farklı çevrimiçi güvenlik konusundaki farkındalığa sahip olmak ve onların bakımında çocuklarla nasıl ilişkili olabileceklerini bilmek.

• Yeni ve gelişmekte olan teknolojiler kullanıldığında iyi uygulamaları modellemek.

• Mümkün olduğunca müfredat ile çevrimiçi güvenlik eğitimini ilişkilendirmek.

• Okul koruma politikalarını ve prosedürlerini takip ederek endişe duyan bireyleri belirlenmek ve önlem alınmak.

• Olumlu öğrenme fırsatlarına vurgu yapmak.

• Bu alanda mesleki gelişim için kişisel sorumluluk almak. Çocukların başlıca sorumlulukları şunlardır: • Çevrimiçi güvenlik politikalarının geliştirilmesine katkıda bulunmak.

• Okulun Kabul Edilebilir Kullanım Politikalarını okumak ve onlara bağlı kalmak.

• Çevrim içi ve çevrimdışı başkalarının hislerine ve haklarına saygı duymak.

• İşler ters giderse, güvenilir bir yetişkinden yardım istemek ve çevrimiçi güvenlik sorunlarıyla karşılaşan diğer kişileri desteklemek.

• Kendilerini ve başkalarını çevrimiçi olarak korumak için sorumluluk almak.

• Yeni ve gelişmekte olan teknolojilerin getirdiği fırsatlar ve risklerle ilgili olarak kendi bilinci ve öğrenimlerinden sorumlu olmak.

• Belli bir teknolojiyi kullanmanın kişisel risklerini değerlendirmek ve bu riskleri sınırlamak için güvenli ve sorumluluk sahibi davranmak. Ebeveynlerin başlıca sorumlulukları şunlardır:

• Okul Kabul Edilebilir Kullanım Politikalarını okumak, çocuklarını bu politikaya bağlı kalmaya teşvik etmek ve uygun olduğunca kendilerinin de bağlı kalmasını sağlamak.
• Çocukların okul ve evde uygun güvenli çevrimiçi davranışlarını pekiştirmek.
• Teknoloji ve sosyal medyanın güvenli ve uygun kullanımında model olmak
• Davranışlarında, çocuğun çevrimiçi olarak zarar görme tehlikesi altında olduğunu gösteren değişiklikleri belirlemek.
• Okul veya diğer uygun kurumlardan, kendileri ve ya çocukları çevrimiçi problem veya sorunlarla karşılaşırsa yardım veya destek istemek.
• Okulun çevrimiçi güvenlik politikalarının oluşturulmasına katkıda bulunmak.
• Öğrenme platformları ve diğer ağ kaynakları gibi okul sistemlerini güvenli ve uygun bir şekilde kullanmak.
• Yeni ve gelişmekte olan teknolojilerin getirdiği fırsatlar ve risklerle ilgili olarak kendi bilinci ve öğrenimlerinden sorumlu olmak. Okul / web sitesinin yönetilmesi
• Web sitesinde iletişim bilgileri okul adresi, e-posta ve telefon numarası olacaktır. Personel veya öğrencilerin kişisel bilgileri yayınlanmayacaktır.
• Okul Müdürü yayınlanan çevrimiçi içerik için genel yayın sorumluluğunu alacak ve bilgilerin doğru ve uygun olmasını sağlayacaktır.
• Web sitesi, erişilebilirlik fikri mülkiyet haklarına saygı, gizlilik politikaları ve telif hakkı da dahil olmak üzere okulun yayın yönergelerine uyacaktır.
• Spam maillerden korunmak için e-posta adresleri çevrimiçi olarak dikkatli bir şekilde yayınlanacaktır.
• Öğrenci çalışmaları öğrencilerin izniyle ya da ebeveynlerinin izniyle yayınlanacaktır.
• Okul web sitesinin yönetici hesabı, uygun bir şekilde güçlü şifreyle şifrelenerek korunacaktır.
• Okul, çevrimiçi güvenlik dahil olmak üzere, toplumun üyeleri için okul web sitesinde korunma hakkında bilgi gönderecektir. Çevrimiçi görüntü ve videolar yayınlama
• Okul, çevrimiçi paylaşılan tüm resimlerin ve videoların okul resim kullanımı politikasına uygun şekilde kullanılmasını sağlayacaktır.
• Okul, resimlerin ve videoların tümünün, veri güvenliği, Kabul Edilebilir Kullanım Politikaları, Davranış Kuralları, sosyal medya, kişisel cihazların ve cep telefonlarının kullanımı gibi diğer politikalar ve prosedürlere uygun şekilde yer almasını sağlayacaktır.
• Görüntü politikasına uygun olarak, öğrencilerin resimlerinin / videolarının elektronik olarak yayınlanmasından önce her zaman ebeveynlerin yazılı izni

İNTERNET KULLANIM SÖZLEŞMESİ

Ebeveynin Taahhüdü

İnternetin çocuklarım için harika bir ortam olabileceğini biliyorum. İnternet ziyaretlerinde güvende olmalarına yardım etmek için üzerime düşeni yapmam gerektiğini de biliyorum. Çocuklarımın bu konuda bana yardımcı olabileceklerini anlayarak, aşağıdaki kurallara uymayı kabul ediyorum:

1. Çocuğumun kullandığı hizmetleri ve web sitelerini yakından tanıyacağım.

2. Çocuklarımın bilgisayar kullanımı ile ilgili makul kurallar ve ilkeler koyacağım, bu kuralları

Konuşup tartışacağım ve hatırlatma notu olarak bilgisayara yakın bir yere asacağım.

3. Çocuğum bana internet üzerinde bulduğu ya da yaptığı "kötü" bir şeyden söz ederse aşırı tepki göstermeyeceğim.

4. Çocuğumun diğer ortamlarda edindiği arkadaşlarını tanımaya çalıştığım gibi, sanal ortamda ve Buddy List (sanal arkadaş listesini düzenlemeyi sağlayan bir modül)'deki "arkadaşlarını" da

Yakından tanımaya çalışacağım.

5. Bilgisayarı evde tüm aile bireylerinin kullandığı ortak bir alana koymaya çalışacağım.

6. Şüpheli ve yasadışı faaliyetler/web sitelerini ilgili makamlara rapor edeceğim.

7. Çocuklar için tavsiye edilen sitelerin bir listesini yapacağım ya da araştırıp bulacağım.

8. Çocuklarımın internet üzerinde hangi siteleri ziyaret ettiğini sıklıkla kontrol edeceğim.

9. İnternette uygunsuz içeriği filtrelemek ve engellemek için seçenekleri araştıracağım.

10. Çocuklarım ile sanal ortamdaki keşifleri hakkında konuşacağım ve elimden geldiği kadar sıkça onlarla birlikte sanal maceralara atılacağım.

Yukarıda yazılanları kabul ediyorum.

Ebeveyn imza (ları) Tarih:


SELÇUKLU İMKB ÖZEL EĞİTİM UYGULAMA OKULU (I. II. III. KADEME)
1994
KONYA