ATAŞEHİR İLÇE MİLLİ EĞİTİM MÜDÜRLÜĞÜ

İstanbul Fuat Sezgin Bilim Ve Sanat Merkezi

e-Güvenlik Politikası

2022-2023

E-GÜVENLİK KURUM POLİTİKASI

Amaçlar ve Politika Kapsamı

İstanbul Fuat Sezgin Bilim ve Sanat Merkezi, 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.

• İstanbul Fuat Sezgin Bilim ve Sanat Merkezi, eğitim standartlarını yükseltmek, başarıyı teşvik etmek, personelin mesleki çalışmalarını desteklemek ve yönetim işlevlerini geliştirmek için toplumun kaliteli İnternet erişimi sunma yükümlülüğüne sahiptir. İstanbul Fuat Sezgin Bilim ve Sanat Merkezi, 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 Kurum tarafından verilen cihazlar için de geçerlidir.

Tüm çalışanların sorumlulukları şunlardır:

• Çevrimiçi güvenlik politikalarının geliştirilmesine katkıda bulunmak.

• Kurum sistemlerinin ve verilerin güvenliğinden sorumlu olmak.

• Yeni ve gelişmekte olan teknolojiler kullanıldığında iyi uygulamaları modellemek.

• Mümkün olduğunca müfredat ile çevrimiçi güvenlik eğitimini ilişkilendirmek.

• Olumlu öğrenme fırsatlarına vurgu yapmak.

• Bu alanda mesleki gelişim için kişisel sorumluluk almak.

Çocukların başlıca sorumlulukları şunlardır:

• Çevrimiçi güvenlik politikalarının geliştirilmesine katkıda bulunmak.

• Çevrimiçi 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.

• Belli bir teknolojiyi kullanmanın kişisel risklerini değerlendirmek ve bu riskleri sınırlamak için güvenli ve sorumluluk sahibi davranmak.

Ebeveynlerin başlıca sorumlulukları şunlardır:

• Çocuklarıyla çevrimiçi güvenlik konularını tartışmak, Kurumun çevrimiçi güvenlik yaklaşımlarını desteklemek ve evde uygun güvenli çevrimiçi davranışları pekiştirmek.

• Teknoloji ve sosyal medyanın güvenli ve uygun kullanımını modellemek.

• Davranışlarında, çocuğun çevrimiçi olarak zarar görme tehlikesi altında olduğunu gösteren değişiklikleri belirlemek.

• Kurum veya diğer uygun kurumlardan, kendileri veya çocukları çevrimiçi problem veya sorunlarla karşılaşırsa yardım veya destek istemek.

• Kurumun çevrimiçi güvenlik politikalarının oluşturulmasına katkıda bulunmak.

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

Çevrimiçi İletişim ve Teknolojinin Daha Güvenli Kullanılması

Kurum Web Sitesinin Yönetilmesi

• Web sitesinde iletişim bilgileri Kurum adresi, e-posta ve telefon numarası olacaktır. Personel veya öğrencilerin kişisel bilgileri yayınlanmayacaktır.

• Kurum 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 Kurumun 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.

• Kurum web sitesinin yönetici hesabı, uygun bir şekilde güçlü şifreyle şifrelenerek korunacaktır. • Kurum, çevrimiçi güvenlik dahil olmak üzere, toplumun üyeleri için Kurum web sitesinde korunma hakkında bilgi gönderecektir. Çevrimiçi görüntü ve videolar yayınlama

• Kurum, çevrimiçi paylaşılan tüm resimlerin ve videoların Kurum resmi kullanımı politikasına uygun şekilde kullanılmasını sağlayacaktır.

• Kurum, resimlerin ve videoların tümünün, veri güvenliği, 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 alınacaktır. İnternetin ve ilgili cihazların uygun ve güvenli kullanımı

• İnternet kullanımı eğitimsel erişimin önemli bir özelliğidir ve tüm çocuklar bütünleşik Kurum müfredatının bir parçası olarak sorunlarını yanıtlamak için stratejiler geliştirmelerini destekleyecek ve onlara yardımcı olacak yaşa ve yeteneğe uygun eğitim alacaklardır.

• Kurumun internet erişimi eğitimi geliştirmek ve genişletmek için tasarlanacaktır.

• İnternet erişim seviyeleri müfredat gerekliliklerini ve öğrencilerin yaş ve yeteneklerini yansıtacak şekilde gözden geçirilecektir.

• Kurumun tüm üyeleri, çocukları korumak için tek başına filtrelemeye güvenmeyeceklerinin farkındadır ve gözetim, sınıf yönetimi ve güvenli ve sorumlu kullanım eğitimi önemlidir.

• Personel üyeleri, web sitelerini, araçlarını ve uygulamalarını sınıfta kullanmadan önce veya evde kullanmayı önerirken daima değerlendirecektir.

• Öğrenciler, bilginin konumlanması, alınması ve değerlendirilmesi becerileri de dahil olmak üzere, İnternette araştırmada etkili kullanımı konusunda eğitilecektir.

• Öğrencilere, okudukları ve / veya gösterilen bilgilerin doğruluğunu kabul etmeden önce eleştirel düşünmeleri öğretilecektir.

• Çevrimiçi materyallerin değerlendirilmesi, her konuda öğretme ve öğrenmenin bir parçasıdır ve müfredatta bir bütün olarak görülür.

Kişisel Cihazların ve Cep Telefonlarının Kullanımı

• İstanbul Fuat Sezgin Bilim ve Sanat Merkezi, mobil teknolojilerle yapılan kişisel iletişimin, çocuklar, personel ve anne- babalar için gündelik yaşamın kabul edilen bir parçası olduğunun farkındadır; ancak, bu tür teknolojilerin Kurumda güvenli ve uygun bir şekilde kullanılmasını gerektirir.

Kişisel cihazların ve cep telefonlarının güvenli bir şekilde kullanılması için beklentiler

• Kişisel cihazların ve cep telefonlarının kullanımı yasaya ve diğer uygun Kurum politikalarına uygun olarak yerine getirilecektir.

• Kuruma getirilen her türlü elektronik cihazın sorumluluğu kullanıcıya aittir. Kurum, bu tür öğelerin kaybı, çalınması veya zarar görmesi konusunda sorumluluk kabul etmez. Kurum, bu tür cihazların potansiyel veya fiili neden olduğu olumsuz sağlık etkileri için sorumluluk kabul etmez.

• Kötüye kullanım veya uygun olmayan mesajların veya içeriğin ceptelefonları veya kişisel cihazlarla gönderilmesi, Kurum idaresi tarafından yasaklanır ve herhangi bir ihlal, disiplin / davranış politikasının bir parçası olarak ele alınacaktır.

• İstanbul Fuat Sezgin Bilim ve Sanat Merkezi tüm üyelerine cep telefonlarını veya cihazlarını kayıp, hırsızlık veya hasardan korumak için adım atmaları önerilir.

• İstanbul Fuat Sezgin Bilim ve Sanat Merkezi tüm üyelerinden, kayboldukları veya çalındığı takdirde yetkisiz aramaların veya hareketlerin telefonlarında veya cihazlarında yapılamayacağından emin olmak için şifreler / pin numaraları kullanmaları önerilir. Parolalar ve pin numaraları gizli tutulmalıdır. Cep telefonları ve kişisel cihazlar paylaşılmamalıdır.

Öğrencilerin kişisel cihazlar ve cep telefonları kullanımı

• Öğrenciler, kişisel cihazların ve cep telefonlarının güvenli ve uygun kullanımı konusunda eğitim alacaklardır.
• Cep telefonları veya kişisel cihazlar, öğrencilerin bir öğretmenin onayını alarak onaylanmış ve yönlendirilmiş

müfredat tabanlı etkinlik kapsamında olmadıkları sürece dersler veya resmi kurum saatlerinde öğrenciler tarafından kullanılamaz.

• Çocukların cep telefonlarını veya kişisel cihazlarını eğitim etkinliğinde kullanımı, kurum idaresi tarafından onaylandığında gerçekleşecektir.

• Özel nedenlerle(hastalık,ulaşım sorunu...) kuruma getirilen cep telefonları sınıf nöbetçi öğrencisi tarafından ilk dersten önce toplanıp,memur odasında her sınıfa ait cep telefonu kutularında saklanacak;günün sonunda öğrenciye teslim edilecektir. • Bir öğrenci ebeveynlerini arama gereği duyduğunda, kurum telefonunu kullanmasına izin verilecektir. • Ebeveynlerin kurum saatlerinde cep telefonuyla çocuklarıyla iletişim kurmamaları, kurum idaresine başvurmaları önerilir. İstisnai durumlarda öğretmenin onayladığı şekilde istisnalara izin verilebilir. • Öğrenciler, telefon numaralarını yalnızca güvenilir arkadaşlarına ve aile üyelerine vermelidirler. • Öğrencilere, cep telefonlarının ve kişisel cihazların güvenli ve uygun bir şekilde kullanımı öğretilecek ve sınırların ve sonuçların farkına varılacaktır. Personelin kişisel cihazlar ve cep telefonları kullanımı • Personelin, kendi kişisel telefonlarını veya cihazlarını, çocukların, gençlerin ve ailelerinin, mesleki bir kapasitede, ortamın içinde veya dışındaki bölgeleriyle bağlantı kurmalarına izin verilmez. Bu konuyu tehlikeye atacak önceden var olan ilişkiler yöneticilerle görüşülecektir.

• Personel, kişisel telefonların ve cihazların herhangi bir şekilde kullanımının daima veri koruma ve ilgili kurum politikası ve prosedürleri uyarınca yerine getirilmesini sağlayacaktır.

• Personel kişisel cep telefonları ve cihazları ders saatlerinde kapatılıp / sessiz moda geçirilir.

• Bluetooth veya diğer iletişim biçimleri ders saatlerinde "gizlenmiş" veya kapalı olmalıdır.

• Bir personel kurum politikasını ihlal ettiği durumlarda disiplin işlemi yapılır.

• Bir personelin, bir cep telefonuna veya kişisel bir cihaza kaydedilen veya saklanan yasadışı içeriğe sahip olduğu veya ceza gerektiren bir suç işlemiş olması durumunda, polise ulaşılacaktır.

• Personelin cep telefonunu veya cihazlarını kişisel olarak kullanmalarını içeren herhangi bir iddiaya kurum yönetim politikasını izleyerek yanıt verilecektir.

Çocukların eğitimi

• Öğrenciler arasında güvenli ve sorumlu internet kullanımının önemi ile ilgili farkındalık yaratmak için bir çevrimiçi güvenlik (e-Güvenlik) müfredatı oluşturulur ve kurumun tamamında yer alır.

• Güvenli ve sorumlu kullanım ile ilgili eğitim internet erişiminden önce yapılacaktır

• Müfredat geliştirme ve uygulama da dahil olmak üzere, kurum çevrimiçi güvenlik politikaları ve uygulamaları yazarken ve geliştirirken öğrenci katkıları aranacaktır.

• İnternetin ve teknolojinin güvenli ve sorumlu kullanımı, müfredatta ve tüm konularda güçlenecektir.

• Kurum, öğrencilerin ihtiyaçlarına uygun olarak çevrimiçi güvenliği geliştirmek için akran eğitimini uygulayacaktır.

Personelin eğitimi

• Çevrimiçi güvenlik (e-Güvenlik) politikası, tüm çalışanların katılımı için resmi olarak sağlanacak ve tartışılacak ve korunma sorumluluğumuzun bir parçası olarak güçlendirilecek ve vurgulanacaktır.

• Kurumun tüm personeline, profesyonel ve kişisel olarak, güvenli ve sorumlu İnternet kullanımı konusunda güncel ve uygun personel eğitimi, düzenli (en az yıllık) temelde çeşitli şekillerde sağlanacaktır.

• Çalışanların tüm üyeleri, çevrimiçi davranışlarının kurumdaki rolü ve itibarını etkileyebileceğinin farkına varacaktır.

• Kurum, çalışanların öğrencilerin yaşlarına ve yeteneklerine göre kullanması gereken yararlı çevrimiçi araçları vurgulamaktadır.

Ebeveynlerin eğitimi

• İstanbul Fuat Sezgin Bilim ve Sanat Merkezi çocukların internetin ve dijital teknolojinin güvenilir ve sorumlu kullanıcıları olabilmesi için ana-babaların oynayacakları önemli bir role sahip olduklarını kabul eder.

• Ebeveynlerin dikkatleri, kurum ağ uygulamaları ve kurum web sitesinde kurum çevrimiçi güvenlik (e-Güvenlik) politikasına ve beklentilerine yönelecektir.

• Çevrimiçi güvenlik konusundaki ebeveynler için bilgi ve rehberlik, ebeveynlere çeşitli biçimlerde sunulacaktır.

• Ebeveynlerin, çevrimiçi olarak çocukları için olumlu davranışları rol modellemeleri teşvik edilecektir.

Çevrimiçi Olaylara ve Koruma sorunlarına yanıt verme

• Kurumun tüm üyeleri, cinsel içerikli mesajlaşma, çevrimiçi / siber zorbalık vb. dahil olmak üzere karşılaşılabilecek çevrimiçi risklerin çeşitliliğinden haberdar edilecektir. Bu, öğrencilere yönelik personel eğitimi ve eğitim yaklaşımları içerisinde vurgulanacaktır.

• Kurumun tüm üyeleri, filtreleme, cinsel içerikli mesajlaşma, siber zorbalık, yasadışı içerik ihlali vb. gibi çevrimiçi güvenlik (e-Güvenlik) endişelerini bildirme prosedürü hakkında bilgilendirilecektir.

• Kurumun tüm üyeleri, gizliliğin öneminden ve endişeleri bildirmek için resmi kurum usullerine uyma ihtiyacından haberdar olmalıdırlar.

• Kurumun tüm üyeleri, çevrimiçi ortamda güvenli ve uygun davranış hakkında hatırlatılacak ve kurum camiasının herhangi bir diğer üyesine zarar vermek, sıkıntı yaşamak veya suç oluşturan herhangi bir içerik, yorum, resim veya video yayımlamamanın önemini hatırlatacaktır.

• Kurum, çevrimiçi güvenlik (e-Güvenlik) olaylarını, uygun olduğunda, kurum disiplini / davranış politikasına uygun olarak yönetir.

• Kurum, ebeveynlere, ihtiyaç duyulduğunda bunlarla ilgili endişeleri bildirir.

• Sorunları çözmek için ebeveynlerin ve çocukların kurumla ortak çalışması gerekir.

EK BİLGİLER : 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 sistem içindeki 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.

Siber Güvenlik kapsamında kurumumuzda Öğretmenlere, Öğrencilere ve idarecilere sürekli aktarılan konu:

Zayıf Parola Oluşturulmaması,

Ortak internet kullanımında zararlı şüpheli sitelere girmeye çalışılmaması,

Şifrenin Öğrencilerle Paylaşılmaması,

Kayıtlı cihazlar dışında başka bir cihazdan erişim sağlanmaması,

urumumuzda Kişisel verilerimizin bilinçsizce toplanmaması, üçük

yaşta sosyal medya kullanılmasına özendirilmemesi,

Bilinçsizce mobil uygulamaların yüklenmemesi,

Sahte Hesaplara tıklanmamasına dikkat etmekteyiz.

Kurum olarak güvenliğimiz çerçevesinde öğrencilerimize yararlı ve zararlı bilginin farkına vardırmak ve zaman yönetiminin farkına vardırmak ana gayelerimizdendir. Yüklenen ve kullanılan programların kullanıcı sözleşmelerini sonuna kadar okumaya özen göstermekteyiz. Kurumumuzda Cep Telefonu Kullanımı ile ilgili öğrencilerimizin ve velilerimiz kafalarındaki soru işaretlerini gidermek adına ilgili yönetmelik maddelerini sizlerle paylaşmayı uygun bulduk. 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.

ÖDÜL VE DİSİPLİN YÖNETMELİĞİ CEP TELEFONU İLE İLGİLİ MADDELER: Disiplin cezasını gerektiren davranışlar MADDE 12 – (1) Cezayı gerektiren davranışlar şunlardır: a) Kınama cezasını gerektiren davranışlar;

18) Bilişim araçlarını, kurum yönetimi ile öğretmenin bilgisi ve izni dışında konuşma yaparak, ses ve görüntü alarak, mesaj ve e-mail göndererek, bunları arkadaşlarıyla paylaşarak eğitim-öğretimi olumsuz yönde etkileyecek şekilde kullanmak, b) Kurumdan kısa süreli uzaklaştırma cezasını gerektiren davranışlar;

8) Bilişim araçları ile yönetici, öğretmen, eğitici personel, memur, diğer görevliler ve ziyaretçiler ile öğrencileri rahatsız edici davranışlarda bulunmak, c) Kurumdan tasdikname ile uzaklaştırma cezasını gerektiren davranışlar;

14) Bilişim araçları ile yönetici, öğretmen, eğitici personel, öğrenci, memur, diğer görevliler ve ziyaretçilere etik olmayan ses, söz ve görüntülerle zarar verici davranışlarda bulunmak, ç) Örgün eğitim dışına çıkarma cezasını gerektiren davranışlar;

14) Bilişim araçları ile toplum değerlerine aykırı zararlı, bölücü, yıkıcı, ahlak dışı ve şiddet içerikli yasak yayınlar bulundurarak kişi ve kurumlarla ilgili ses, söz ve görüntüler alıp bunları çoğaltmak, sanal ortamlarda dinlemek, dinlettirmek, izlemek, izlettirmek, yaymak ve ticaretini yapmak," Görüldüğü üzere cep telefonunun yanlış amaçlar doğrultusunda kullanımı ile ilgili yönetmelik maddeleri açık olup, bu konuda velilerimizin gerekli uyarı ve tavsiyeleri öğrencilerine duyurmaları önemle rica olunur.

Siber Zorbalık ve Önleyici Çalışmalar

SİBER ZORBALIK

Zorbalık nedir?

Zorbalık konusunda net bir tanım olmamakla birlikte; aralarında güç dengesizliği olan kişilerden, güçsüzün, güçlünün saldırganca ve kasıtlı zarar verme niteliği bulunan davranışlarına tekrarlı olarak ve birçok kez maruz kalması durumuna zorbalık denir. Siber zorbalık nedir? Bir ya da birden fazla kişinin elektronik iletişim araçlarını kullanmak suretiyle belirli bir zaman içerisinde ve sürekli olarak, kendisini savunma gücüne sahip olmayan bir kişiye yönelik gerçekleştirilen kasıtlı saldırgan davranışlardır. Siber zorbalık davranışları nasıl gerçekleştirilmekte? Bu davranışların başında zorbanın, kurbanı, elektronik iletişim araçları yoluyla tehdit etmesi ya da kurbana yönelik kötü sözler içeren mesajlar göndermesi gelmektedir. Bazen de mağdur hakkında internet ortamında dedikodu yaparak ya da mağduru rahatsız edecek özel resim ve bilgiler yayma yoluyla gerçekleştirilmektedir. Yaygın siber zorbalık davranışlarından biride zorbanın internet ortamından kendisini mağdur gibi tanıtıp onun adına başkalına zorbalık yapmasıdır. Bu tür davranışlar, mağdurun cep telefonu ya da elektronik posta hesabını kullanarak gerçekleştirdiği görülmektedir. Bunlara ek olarak isimsiz çağrılar, virüslü e-postalar ve bir kişi ya da bir grubu karalamak için kısa mesaj ya da e-postaların gönderilmesi de diğer siber zorbalık davranışları arasında yer almaktadır. Siber zorbalığın nedenleri nelerdir? Başka kişilere zarar vermenin kolaylığı, düşük maliyet, kolay erişim, kimliğini gizleme kolaylığı, akıl sağlığı sorunu, az gelişmiş sosyal beceriler, düşük benlik saygısı, yüksek sosyal kaygı, saldırganlık, uygun olmayan davranışların model alınması, yetersiz ebeveyn-çocuk etkileşimi, internet kullanımında yetersiz süpervizyon. Siber zorbalık çeşitleri nelerdir? İki çeşit siber zorbalık bulunmaktadır. Elektronik zorbalık: Olayın daha çok teknik yönünü içermektedir. Bu zorbalık kişilerin şifrelerini ele geçirmek, web sitelerini heklemek, spam içeren mailler göndermek ya da bulaşıcı mailler göndermek gibi teknik olayları içerir. Bireysel yapılabileceği gibi birçok kişi tarafından organize bir şekilde aynı anda da yapılabilir.

E-iletişim zorbalığı: Olayın daha çok psikolojik yönünü içerir. Bilgi ve iletişim teknolojilerini kullanarak kişileri sürekli rahatsız etme, isim takma, dedikodu yapma internet üzerinden kötüleme ve hakaret etme ya da kişinin rızası olmadan fotoğraflarını yayınlama gibi ilişkisel saldırı davranışlarını içerir. Siber zorbalığın meydana geldiği en yaygın siber ortam hangisidir? Neden? Siber zorbalığın en yaygın olduğu siber ortam facebook adlı sosyal paylaşım sitesidir. Araştırmalar, gençlerin giderek artan oranda internet kullandıklarını hatta bazılarının internet bağımlısı haline geldiklerini belirtmektedir. Şüphesiz bu bağımlılığın en büyüğü de facebooktur. Facebook ve benzeri paylaşım sitelerinin, bireylerin siber ortamda tanıştıkları, anlık ileti göndermek suretiyle sohbet ettikleri, sesli ve görsel beğenileri paylaştıkları sosyal bir platforma dönüşmüş olması siber zorbalığı yaygınlaştırmaktadır. Aynı zamanda bu sitelerde zorbanın mağdur ile yüzyüze iletişim halinde olmamalarının verdiği göreceli rahatlık kullanımı artırmaktadır. Siber zorbalığın öğrenciler arasında yaygınlaşmasının temel nedenleri nelerdir? Bu noktada bozulan arkadaşlık ilişkileri dikkat çekmektedir. Özellikle duygusal ilişki yaşayan gençlerden bir bölümünün ilişkinin bitmesi sonucunda intikam amaçlı olarak bölümünün ilişkinin bitmesi sonucunda intikam amaçlı olarak siber zorbalık yaptığı görülmektedir. Diğer yandan bazı öğrencilerin kıskançlık, bazılarının ise fazla farklı alt kimliklere yönelik sahip oldukları ön yargılar ve bazı öğrencilerin kurbanı, grup dışına itmek ya da grup içerisinde kendi yerini korumak amacıyla da siber

zorbalığa yöneldikleri görülmektedir. Siber zorbalıkla nasıl baş edilir? Siber zorbalığın giderek yaygınlaştığı ve önemli bir sosyal soruna dönüştüğü görülmektedir. Bu nedenle de öncelikli olarak öğrencileri siber zorbalığa iten nedenlerin daha geniş gruplar üzerinde yapılacak çalışmalarla incelenmesinin yerinde olacağı düşünülmektedir. Bununla birlikte öğrenci, veli, öğretmen ve kurum yöneticileri başta olmak üzere eğitim sürecinin tüm paydaşlarının, hayatın her alanında etkisi ve kapsamı giderek genişleyen siber iletişim konusunda eğitilmeleri gerekmektedir. Özellikle paydaşların, bilişim suçları ve bu suçlara karşılık gelen idari ve adli cezalar konusunda bilgilendirilmesi önemlidir. Zorbalık mağdurlarının çeşitli tür ve yoğunlukta psikolojik bozukluklar yaşadıkları görülmektedir. Bu nedenle mağdurların psikolojik destek almalarının sağlanması gerekmektedir. Sağlanacak sosyal desteğin mağdurların kendilerini daha iyi hissetmelerine katkı getirdiği gözlenmektedir.

Siber zorbalık duyarlılığı?

İnternet, cep telefonu gibi siber araçların kullanımı esnasında zorbaca davranışlara maruz kalmaya yol açabilecek davranışlardan uzak durma, bu tür tehditlerin varlığından haberdar olma ve tedbir alma, bu konuda bilinçlenme, tehdit oluşabilecek uyarıcıları fark etmeye yönelik dikkati yüksek tutma davranışlarıdır. Siber zorbalık çocukların yaşamında ne gibi kötü etkiler bırakmaktadır? Böyle bir zorbalıkla karşılaşan çocukların hayata dair yeterli donanıma ve deneyime sahip olmadıklarını düşündüğümüzde onların ne denli korku içinde olduklarını anlamak hiç de zor olmaz. Çocuklar içine düştükleri durumu kolaylıkla ailelerine açıklayamıyorlar, onların zarar görecekleri korkusundan dolayı korkunç bir kısır döngü yaşayarak, kendi hayatlarından vazgeçmeye kadar varan olumsuz sonuçlara yönelebiliyorlar.

KAYNAKÇA

http://internetzorbalig.blogspot.com.tr/
http://www.cyberbullyinginstitute.org/
http://www.siberzorbalik.com/

EK-4 AİLE ÇOCUK 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 bilgisayarın yanına 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:

Ailemin bu kurallara göre yaşamayı kabul ettiğini anlıyorum ve interneti benimle birlikte keşfetmeleri için aileme yardım etmeyi kabul ediyorum.

Çocuğun imzası Tarih

Çocuğun Taahhüdü

İnternetin benim için harika bir ortam olabileceğini biliyorum. İnternet ziyaretlerimde güvende olmama yardım edecek kurallara uymamın benim için önemli olduğunu da biliyorum.

Aşağıdaki kurallara uymayı kabul ediyorum:

1. Kendime ya da ailemin diğer bireylerine ait kişisel bilgileri açık etmeyecek şekilde, kendim için güvenli ve makul bir ekran adı seçeceğim.

2. Şifremi ailem dışında herkesten gizli tutacağım. Ailemin onayı olmadan başka e-posta hesapları açmayacağım.

3. Sanal profilime kişisel bilgilerimi dahil etmeyeceğim. Kendime ya da ailemin diğer bireylerine ait kişisel bilgileri - herhangi bir yoldan ve herhangi bir formatta - sanal olarak ya da sanal ortamda tanıştığım biriyle paylaşmayacağım. İsim, adres, telefon numarası, yaş ya da kurum adı bu kapsama girmekle birlikte, kişiler bilgiler sadece bunlarla sınırlı değildir.

4. Bana nasıl davranılmasını istiyorsam ben de başkalarına karşı öyle davranacağım.

5. Sanal ortamda iken, düzgün ve saygılı bir dil kullanmak da dahil, görgü kurallarına uygun şekilde davranacağım. Kavga başlatmayacağım, tehdit içeren ya da kötü sözcükler kullanmayacağım.

6. Çevrimiçi oldukları halde kendilerini sanki değillermiş gibi gösteren kişiler olabileceğini bildiğim için, kişisel güvenliğimi her şeyden önde tutacağım.

7. Sanal ortamda tanıştığım kişiler hakkında ebeveynlerime karşı dürüst olacağım, ve her defasında onların sormalarını beklemeden, kendim bu kişilerden söz edeceğim. Ebeveynlerimin onaylamadığı birinden gelecek e-posta ya da anlık iletilere yanıt vermeyeceğim.

8. Kötü, iğrenç, ya da adi şeyler gördüğüm/okuduğum takdirde, bu durumun tekrarlamasını engellemeleri için hemen oturumu kapatıp ebeveynlerime anlatacağım.

9. Kötü sitelere ait resimler/linkler ya da kötü dille yazılmış e-posta/anlık iletiler alırsam; katılımcıların küfür, adi ya da nefret sözcükleri içeren dil kullandığı bir sohbet odasına girersem derhal ebeveynlerime söyleyeceğim.

10. Sanal ortamda tanıştığım birine, ebeveynlerimin onayı olmadan, hiçbir şey göndermeyeceğim. Sanal ortamda tanıştığım birinden herhangi bir şey aldığım takdirde ise, derhal ebeveynlerime söyleyeceğim (bu durumda o kişinin elinde kişisel bilgilerim var demektir).

11. Sanal ortamda tanıştığım birileri - özellikle ebeveynlerimin hoşlanmayacakları ya da onaylamayacakları bir şey yapmamı istiyorlarsa, bunu yapmayacağım.

12. Ebeveynlerimin onayını almadan ya da yanımda bir ebeveyn olmadan, sanal ortamda tanıştığım birine telefon etmeyeceğim, posta yoluyla mektup yollamayacağım ya da buluşmaya gitmeyeceğim.

13. Ebeveynlerimin sanal ortamda geçireceğim zamanı denetleyeceklerini, girdiğim siteleri izlemek ya da sınırlamak için bir yazılım kullanacaklarını anlıyorum. Beni sevdikleri ve korumak istedikleri için böyle davranıyorlar.

14. Birlikte eğlenmek ve yeni şeyler öğrenmek için, ebeveynlerime internet hakkında daha fazla şey öğreteceğim.

Yukarıda yazılanları kabul ediyorum.

Çocuğun imzası Tarih

Bu kurallara uyulmasını sağlayarak çocuğumun sanal ortamdaki güvenliğini koruyacağıma söz veriyorum. Çocuğum tehlikeli durumlar ile karşılaşıp bana anlatırsa; kimseyi suçlamadan her durumda olgun ve sağduyulu bir şekilde davranacağım, ve gelecekte daha güvenli bir internet deneyimi yaşaması için çocuğumla birlikte durumu sakin bir şekilde ele alacağım.

Ebeveyn imza (ları) Tarih

EK-6 GÜVENLİ İNTERNET HİZMETİ BAŞVURUSU

Güvenli İnternet Hizmeti almak için internet servis sağlayıcınızın internet sitesi üzerinden işlem yapabilir ya da servis sağlayıcınıza telefon edebilirsiniz. Aynı yolla, istediğiniz zaman, ücretsiz olarak profilinizi değiştirebilir ya da hizmet almayı bırakabilirsiniz.