E GÜVENLİK POLİTİKAMIZ

İLETİŞİM BİLGİLERİ

TELEFON:
0 (312) 270 23 60

WEB SİTESİ:
http://
sincan100yililkokulu.meb.k12.tr/

E-POSTA:
711583@mebk12tr

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.

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 kişiye 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 okul 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-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. Aşağıda yazılan örneklerdeki gibi bir kısa mesaj ile de Güvenli İnternete geçebilirsiniz. "Hizmet No" yazan kısımlara Servis Sağlayıcınızın size verdiği abonelik numaranızı yazarak, Servis sağlayıcınıza bildirdiğiniz numarayla mesaj atabilirsiniz. İşletmeci Çağrı Merkezi Online İşlem Merkezi Çocuk Profili için Aile Profili için AVEA 444 1 500 avea.com.tr EVET -> 3398 EVET -> 3399 TURKCELL 444 0 532 turkcell.com.tr GUVENLI COCUK -> 7777 * GUVENLI AILE -> 7777 * VODAFONE 444 0 542 vodafone.com.tr COCUK ->7005 AILE ->7005 TTNET 444 0 375 ttnet.com.tr COCUK -> 6606 AILE -> 6606 TURKSAT 444 0 126 turksat.com.tr COCUK HİZMETNO -> 5126 AILE HİZMETNO - > 5126

1. OKULUMUZ, E-güvenliğin (e-Güvenlik), bilgisayarlar, tabletler ve cep telefonları gibi teknolojiyi kullanırken, dijital dünyadaki çocukların ve yetişkinlerin korunması için vazgeçilmez bir unsur olduğuna inanmaktadır. Ve bu doğrultuda gerekli

çalışmalar yapılmaktadır.

2. OKULUMUZ, Sanal platformların ve bilgi iletişim teknolojilerinin günlük yaşamın önemli bir parçası olduğuna inanmakta olup çocukların sanal ortamda karşılaştıkları riskleri yönetmeleri ve bunlara tepki vermek ve stratejiler geliştirmenin yollarını öğrenmeleri için destekleyici çalışmalar yapmaktadır.
3. OKULLARIMIZ, eğitim standartlarını yükseltmek, başarıyı teşvik etmek, personelin mesleki çalışmalarını desteklemek ve yönetim işlevlerini geliştirmek için toplumun kaliteli İnternet erişimi sunma yükümlülüğüne sahiptir
4. OKULLARIMIZ, tüm çocuklarımızın ve personellerimizin sanal ortamlarda potansiyel zararlardan korunmasını sağlamakla sorumludur.
5.
6. **OKULUMUZDA, E-Güvenlik politikasının amacı;**

OKULUMUZDA, güvenli ve güvenli bir ortam olduğundan emin olmak için, toplumun tüm üyelerinden beklenen ana ilkeleri, güvenli ve sorumlu kullanım teknolojisi ile ilgili olarak tanımlamak.

OKULUMUZDA, topluluğunun tüm üyelerini çevrimiçi olarak korumak ve güvenliğini sağlamak.

Teknolojinin potansiyel riskleri ve yararları konusunda SİNCAN 100. YIL İLKOKULU topluluğunun tüm üyelerinde farkındalık yaratmak.

Tüm personelin güvenli ve sorumlu bir şekilde çalışmasını sağlamak, olumlu davranışları online olarak modellemek ve teknolojiyi kullanırken kendi standartlarını ve uygulamalarını yönetme gereksiniminin farkında olmak.

Okuldaki tüm üyeler tarafından bilinen çevrimiçi güvenlik endişelerine yanıt verirken açıkça kullanılacak prosedürleri tanımlamak.

Bu politika, yönetim organı, öğretmenler, destek personeli, harici yükleniciler, ziyaretçiler, gönüllüler ve okul adına hizmet veren veya bunları yerine getiren diğer kişiler (toplu olarak bu politikada ´personel´ olarak anılacaktır) dahil olmak üzere tüm personel için geçerlidir) yanı sıra çocuklar ve ebeveynler.

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.

6. **Tüm çalışanların kilit sorumlulukları şunlardır:**
    - Çevrimiçi güvenlik politikalarının geliştirilmesine katkıda bulunmak.
    - Kabul Edilebilir Kullanım Politikalarını (AUP´lar) 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 modelleme
- Mümkün olduğunca müfredat ile çevrimiçi güvenlik eğitimini ilişkilendirme.
- Okul koruma politikalarını ve prosedürlerini takip ederek endişe duyan bireylerin belirlenmesi ve uygun önlem alınması.
- Çevrimiçi güvenlik konusunu ne zaman ve ne kadar içte ve dışta tırmanacağınızı bilmek.
- Çevrimiçi güvenlik konularda, dahili ve harici olarak, uygun desteğin işaretini koymak.
- Kişisel ve kişisel teknoloji kullanımlarında, hem açık hem de kapalı alanda profesyonel bir davranış seviyesinin korunması.
- Olumlu öğrenme fırsatlarına vurgu yapmak.
- Bu alanda mesleki gelişim için kişisel sorumluluk almak.

7. **Çocukların ve gençlerin başlıca sorumlulukları şunlardır:**
    - Çevrimiçi güvenlik politikalarının geliştirilmesine katkıda bulunmak.
    - Okulun Kabul Edilebilir Kullanım Politikalarını (AUP ´lar) 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.

8. **Bireysel yaşlarına, yeteneklerine ve zayıf yönlerine uygun bir seviyede:**
    - 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.

9. **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.
    - Çocuklarıyla çevrimiçi güvenlik konularını tartışmak, okulun 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.
    - 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.

10. **Çevrimiçi İletişim ve Teknolojinin Daha Güvenli Kullanımı**
11. **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, ulusal ve/veya uluslararası projelerde 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 alınacaktır.

- **Kullanıcılar**
    - Öğrenciler, bir video konferans araması veya mesajı hazırlamadan veya cevaplamadan önce bir öğretmenin izin isteyecektir.
    - Video konferans, öğrencilerin yaşı ve yeteneği için uygun bir şekilde denetlenecek.
    - Velilerin rızası, çocuklar video konferans faaliyetlerine 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 verilecektir.
    - Eğitimsel video konferans servisleri için özel oturum açma ve şifre bilgileri yalnızca personellere verilecek ve gizli tutulacak.

- **İçerik**
    - Bir video konferans dersi kaydederken, tüm siteler ve katılımcılar tarafından yazılı izin alınacaktır. Konferansın başlangıcında kayıt nedeni belirtilmeli ve video konferans kaydı tüm taraflara açık olmalıdır. Kaydedilen malzemeler güvenli bir

şekilde saklanacaktır.
    - Üçüncü taraf materyalleri dahil edilecekse, okul üçüncü şahsın fikri mülkiyet haklarını ihlal etmekten kaçınmak için bu kaydın kabul edilebilir olup olmadığını kontrol edecektir.
    - Okul, bir video konferansa katılmadan önce diğer konferans katılımcılarıyla diyalog kuracak. Okul değilse, okul sınıf için uygun olan materyali teslim aldığını kontrol edecektir.
- İnternetin ve ilgili cihazların uygun ve güvenli derslik kullanımı
- İnternet kullanımı eğitimsel erişimin önemli bir özelliğidir ve tüm çocuklar bütünleşik okul müfredatının bir parçası olarak sorunlarını yanıtlamak için stratejiler geliştirmelerini destekleyecek ve onlara yardımcı olacak yaşa ve yeteneğe uygun eğitim alacaklardır.
- Okulun internet erişimi eğitimi geliştirmek ve genişletmek için tasarlanacaktır.
- İnternet erişim seviyeleri müfredat gerekliliklerini ve öğrencilerin yaş ve yeteneklerini yansıtacak şekilde gözden geçirilecektir.
- Çalışanların tüm üyeleri, çocukları korumak için tek başına filtrelemeye güvenmeyeceklerinin farkındadır ve gözetim, sınıf yönetimi ve güvenli ve sorumlu kullanım eğitimi önemlidir.
- İçerik;Öğrencilerin yaşlarına ve yeteneklerine uygun olacaktır.
- Tüm okula ait cihazlar, okulun Kabul Edilebilir Kullanım Politikasına uygun olarak ve uygun güvenlik ve güvenlik önlemleri alınarak kullanılacaktır.
- 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.
- Okul, personelin ve öğrencilerin İnternet´ten türetilen materyallerin telif hakkı yasalarına uygun olmasını ve bilgi kaynaklarını kabul etmesini sağlayacaktır.
- Öğrencilere, okudukları ve ya 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.
- Okul, öğrencileri ve çalışanlarımızın güvenli ve gizli bir ortamda iletişim kurmalarını ve işbirliği yapmalarını sağlamak için interneti kullanmaktadır.

- **Kişisel Cihazların ve Cep Telefonlarının Kullanımı**
    - Cep telefonlarının ve çocukların, gençlerin ve yetişkinler arasındaki diğer kişisel cihazların yaygın bir şekilde kullanılması, tüm üyelerin SİNCAN 100.YIL İLKOKULU topluluğunun cep telefonlarının ve kişisel cihazların sorumlu bir şekilde kullanılmasını sağlamak için gerekli adımları atmalarını gerektirir.
    - SİNCAN 100.YIL İLKOKULU, mobil teknolojilerle yapılan kişisel iletişimin, çocuklar, personel ve anne-babalar için gündelik yaşamın kabul edilen bir parçası olduğunun farkındadır; ancak, bu tür teknolojilerin okulda 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 okul politikalarına uygun olarak yerine getirilecektir.
    - Sahaya getirilen her türlü elektronik cihazın sorumluluğu kullanıcıya aittir. Okul, bu tür öğelerin kaybı, çalınması veya zarar görmesi konusunda sorumluluk kabul etmez. Okul, bu tür cihazların potansiyel veya fiili neden olduğu olumsuz sağlık etkileri için sorumluluk kabul etmez.
    - Kötüye kullanım veya uygun olmayan mesajların veya içeriğin cep telefonları veya kişisel cihazlarla gönderilmesi, topluluğun herhangi bir üyesi tarafından yasaklanır ve herhangi bir ihlal, disiplin / davranış politikasının bir parçası olarak ele alınacaktır.
    - SİNCAN 100.YIL İLKOKULU topluluğunun tüm üyelerine cep telefonlarını veya cihazlarını kayıp, hırsızlık veya hasardan korumak için adım atmaları önerilir.
    - SİNCAN 100.YIL İLKOKULU topluluğunun tüm üyelerinden, kayboldukları veya çalındığı takdirde yetkisiz aramaların veya hareketlerin telefonlarında veya cihazlarında yapılamayacağından emin olmak için şifreler / pim numaraları kullanmaları önerilir. Parolalar ve pin numaraları gizli tutulmalıdır. Cep telefonları ve kişisel cihazlar paylaşılmamalıdır.
    - SİNCAN 100.YIL İLKOKULU topluluğunun tüm üyelerine, cep telefonlarının ve kişisel cihazlarının saldırgan, küçümseyen veya başka şekilde okul / ayar politikalarına aykırı düşen herhangi bir içerik

içermediğinden emin olmaları önerilir.

- **Öğrencilerin kişisel cihazlarını ve cep telefonlarını kullanımı**

- Öğrenciler, kişisel cihazların ve cep telefonlarının güvenli ve uygun kullanımını velinin izni ve onayı, okul idaresinin bilgisi ve öğretmenin denetiminde kullanabilecektir.
- Bilişim araçlarını, okul 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 aynı zamanda okul ders saatleri içerisinde telefon bulundurmak kesinlikle yasaktır.
- Çocukların cep telefonlarının ve kişisel cihazların tüm kullanımları, kabul edilebilir kullanım politikasına uygun olarak gerçekleşecektir.
- Cep telefonları veya kişisel cihazlar, öğrencilerin öğretmeninin onayını alarak onaylanmış ve yönlendirilmiş müfredat tabanlı etkinlik kapsamında olmadıkları sürece dersler veya resmi okul saatlerinde öğrenciler tarafından kullanılamaz.
- Çocukların cep telefonlarını veya kişisel cihazlarını eğitim etkinliğinde kullanımı, okul idaresi tarafından onaylandığında gerçekleşecektir.
- Bir öğrenci ebeveynlerini arama gereği duyduğunda, okul telefonunu kullanmasına izin verilecektir.
- Ebeveynlerin okul saatlerinde cep telefonuyla çocuklarıyla iletişim kurmamaları, okul idaresine başvurmaları önerilir. İstisnai durumlarda öğretmenin onayladığı şekilde istisnalara izin verilebilir.
- Öğrenciler, varsa 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.
- Öğrencinin kişisel cihazında veya cep telefonunda bulunan materyalin yasadışı olabileceği veya cezai bir suçla ilgili kanıt sağlayabileceğinden şüpheleniliyorsa, cihaz daha ayrıntılı araştırma için polise teslim edilir.

- **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, çocukların fotoğraflarını veya videolarını çekme işini okul etkinlikleri, projeleri ve etkinlikleri için cep telefonları, tabletler veya kameralar gibi kişisel cihazları kullanmamalı eğer gerekiyorsa yalnızca bu amaçla işle sağlanan ekipmanı kullanır.
    - Personel herhangi bir kişisel cihazı doğrudan çocuklarla kullanmaz ve ders / eğitim etkinlikleri sırasında yalnızca okul tarafından sağlanan ekipmanı kullanır.
    - Personel, kişisel telefonların ve cihazların herhangi bir şekilde kullanımının daima veri koruma ve ilgili okul 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.
    - Acil durumlarda okul idaresi tarafından izin verilmemişse, kişisel cep telefonları veya cihazları öğretim dönemleri boyunca kullanılamaz.
    - Personel, cep telefonları ve kişisel cihazlar üzerinden sitede satın alınan içeriğin profesyonel rolü ve beklentileri ile uyumlu olmasını sağlayacaktır.
    - Bir personel okul 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 okul yönetim politikasını izleyerek yanıt verilecektir.

- **Ziyaretçiler kişisel cihazların ve cep telefonlarının kullanılması**
    - Ebeveynler ve ziyaretçiler, okulun kabul edilebilir kullanım politikasına uygun olarak cep telefonlarını ve kişisel cihazları kullanmalıdır.
    - Fotoğraflar veya videolar çekmek için ziyaretçiler ve ebeveynler tarafından cep telefonlarının veya kişisel cihazların kullanılması, okul resim kullanımı politikasına uygun olarak gerçekleştirilmelidir.
    - Okul, ziyaretçilere kullanım beklentilerini bildirmek

için uygun tabela ve bilgileri sağlayacak ve sunacaktır.
    - Personelin uygun ve güvenli olduğunda sorunlara karşı çıkması beklenir ve her zaman ziyaretçilerin herhangi bir ihlalini idareye bildirecektir.

- **Çocukların katılımı ve eğitimi**
    - Öğrenciler arasında güvenli ve sorumlu internet kullanımının önemi ile ilgili farkındalık yaratmak için bir çevrimiçi güvenlik (e-Güvenlik) müfredatı oluşturulur ve okulun tamamında yer alır.
    - Güvenli ve sorumlu kullanım ile ilgili eğitim internet erişiminden önce yapılacaktır.
    - Müfredat geliştirme ve uygulama da dahil olmak üzere okul çevrimiçi güvenlik politikaları ve uygulamaları yazarken ve geliştirirken öğrenci katkıları aranacaktır.
    - Öğrenciler, Kabul Edilebilir Kullanım Politikasını, yaşlarına ve yeteneklerine uygun bir şekilde okumak ve anlamak için desteklenecektir.
    - Tüm kullanıcılara ağ ve internet kullanımının izleneceği bildirilecektir.
    - Çevrimiçi güvenlik (e-Güvenlik) PSHE, SRE, Citizenshipand Computing / BİT programlarına dahil edilecek ve hem güvenli okul hem de evde kullanımını kapsayacaktır.
    - Kabul Edilebilir Kullanım beklentileri ve Posterler, Internet erişimi olan tüm odalarda yayınlanacaktır.
    - İnternetin ve teknolojinin güvenli ve sorumlu kullanımı, müfredatta ve tüm konularda güçlenecektir.
    - Dışarıdan destek, okulların dahili çevrimiçi güvenlik (e-Güvenlik) eğitim yaklaşımlarını tamamlamak ve desteklemek için kullanılacaktır.
    - Okul, öğrencilerin teknolojiyi olumlu şekilde kullandıklarını ödüllendirecektir.
    - Okul, öğrencilerin ihtiyaçlarına uygun olarak çevrimiçi güvenliği geliştirmek için akran eğitimini uygulayacaktır.

- **Personelin katılımı ve eğitimi**
    - Çevrimiçi güvenlik (e-Güvenlik) politikası, tüm çalışanların katılımı için resmi olarak sağlanacak ve tartışılacak ve korunma sorumluluğumuzun bir parçası olarak güçlendirilecek ve vurgulanacaktır.
    - Personel, İnternet trafiğinin izlenebileceğini ve tek

bir kullanıcıya kadar izlenebileceğinin farkında olacak. 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 tüm üyeleri, çevrimiçi davranışlarının okuldaki rolü ve itibarını etkileyebileceğinin farkına varacaktır. Mesleği veya kurumu çürüme durumuna düşürdüğü veya profesyonel yeteneklerine güvenini kaybetmiş bir şeyin bulunduğu düşünülürse, kamusal, disiplin veya hukuki önlemler alınabilir.
    - Filtreleme sistemlerini yönetme veya BİT kullanımını izleme sorumluluğu taşıyan personelin üyeleri, Liderlik Ekibi tarafından denetlenecek ve sorunları veya endişeleri bildirmek için açık prosedürlere sahip olacaklar.
    - Okul, çalışanların öğrencilerin yaşlarına ve yeteneklerine göre kullanması gereken yararlı çevrimiçi araçları vurgulamaktadır.

- **Ebeveynlerin katılımı ve eğitimi**
    - SİNCAN 100.YIL İLKOKULU, çocukların internetin ve dijital teknolojinin güvenilir ve sorumlu kullanıcıları olabilmesi için ana-babaların oynayacakları önemli bir role sahip olduklarını kabul eder.
    - Ebeveynlerin dikkatleri, okul açıklamaları ve okul web sitesinde okul çevrimiçi güvenlik (e-Güvenlik) politikasına ve beklentilerine yönelecektir.
    - Okullarımızın bir parçası olarak ebeveynlerin çevrimiçi güvenlik bilgilerini okumaları istenecektir.
    - Ebeveynler, Okula Kabul Edilebilir Kullanım Politikasını okumaya ve çocuklarıyla etkilerini tartışmaya teşvik edilecektir.
    - 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**
    - Okulun 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.

- Okulun tüm üyeleri, filtreleme, cinsel içerikli mesajlaşma, siber zorbalık, yasadışı içerik ihlali vb. gibi çevrimiçi güvenlik (e-Güvenlik) endişelerini bildirme prosedürü hakkında bilgilendirilecektir.
- Dijital Abone Hattı (DSL), daha sonra kaydedilecek olan çocuk koruma endişelerini içeren herhangi bir çevrimiçi güvenlik (e-Güvenlik) olayı hakkında bilgilendirilecektir.
- İnternet´in yanlış kullanımı ile ilgili şikâyetler, okulun şikâyet prosedürleri kapsamında ele alınacaktır.
- Çevrimiçi / siber zorbalık ile ilgili şikayetler, okulun zorbalık karşıtı politikası ve prosedürü kapsamında ele alınacak
- Personelin yanlış kullanımı ile ilgili herhangi bir şikayet okul müdürüne yönlendirilecektir
- Okul şikayet prosedürü öğrencilere, velilere ve personele bildirilecektir.
- Şikayet ve ihbar prosedürü personele bildirilecektir.
- Okulun tüm üyeleri, gizliliğin öneminden ve endişeleri bildirmek için resmi okul usullerine uyma ihtiyacından haberdar olmalıdırlar.
- Okulun tüm üyeleri, çevrimiçi ortamda güvenli ve uygun davranış hakkında hatırlatılacak ve okul camiasının herhangi bir diğer üyesine zarar vermek, sıkıntı yaşamak veya suç oluşturan herhangi bir içerik, yorum, resim veya video yayımlamamanın önemini hatırlatacaktır.
- Okul, çevrimiçi güvenlik (e-Güvenlik) olaylarını, uygun olduğunda, okul disiplini / davranış politikasına uygun olarak yönetir.
- Okul, ebeveynlere, ihtiyaç duyulduğunda bunlarla ilgili endişeleri bildirir.
- Herhangi bir soruşturma tamamlandıktan sonra okul bilgi alacak, öğrenilen dersleri belirleyecek ve değişiklikleri gerektiği gibi uygulayacaktır.
- Sorunları çözmek için ebeveynlerin ve çocukların okulla ortak çalışması gerekir.