

ESAFETYLABEL.EU



For safer schools!

Okçu Musa İlkokulu Güvenlik Politikası 2022

Okul eSafety Politikaları hızla gelişmiştir, çünkü paydaşlar günümüzde okuldan çok çeşitli şekillerde internete erişebilmektedir. Günlük hayatımızın bir parçası olarak hepimiz dijital teknolojilerle yaşıyoruz. Çocuklarımızın dijital teknolojiler aracılığıyla mevcut olan fırsatları en iyi nasıl kullanacaklarını bilmelerini sağlamak için, artık bunları nasıl kullanacaklarını bilmek ve anlamak gerekiyor. Bunun mümkün olan en güvenli ve en güvenli ortamda yapılmasını sağlamak için, evde, okulda ya da dışarıda ya da arkadaşlarıyla ya da yalnız olduğu zaman, tüm okulların açık ve özlü bir Okul Politikasına sahip olması gerekmektedir. eSafety'in tüm yönlerine.

1.Çevrimiçi Güvenlik Kurallarını Yaratmak

1.1 Amaçlar ve politika

kapsamı Tüm ayarlar

için uygun

1.1. Olası ifadeler:

* Okçu Musa İlkokulu çevrimiçi güvenliğin (e-Güvenlik), bilgisayar,

tablet, cep telefonu veya oyun konsolu gibi teknolojileri kullanırken dijital dünyadaki çocukların ve yetişkinlerin korunmasının temel bir unsuru olduğuna inanmaktadır.

*Okçu Musa İlkokulu internet ve bilgi iletişim teknolojilerinin günlük hayatın önemli bir parçası olduğunu, dolayısıyla çocukların riskleri yönetmek ve bunlara yanıt vermek için stratejiler geliştirmeyi öğrenebilmeleri için desteklenmeleri ve çevrimiçi olarak esneklik geliştirmeleri için yetkilendirilmeleri gerektiğini destekliyor. .

* Okçu Musa İlkokulu eğitim standartlarını yükseltmek, başarıyı desteklemek, personelin profesyonel çalışmalarını desteklemek ve yönetim işlevlerini geliştirmek için topluluğa kaliteli internet erişimi sağlama görevine sahiptir.

* Okçu Musa İlkokulu tüm çocukların ve personelin çevrimiçi olarak potansiyel zararlardan korunmalarını sağlamak için açık bir görev olduğunu belirtir.

* Okçu Musa İlkokulu çevrimiçi güvenlik politikasının amacı:

Okçu Musa İlkokulunda, öğrencilerimizi e-güvenlik konularında eğitmek zorunda olduğumuz sorumluluğu anlıyoruz; internetin ve ilgili teknolojileri kullanırken sınıfın bağlamında ve ötesinde, hem güvenli hem de yasal kalmalarını sağlamak için uygun davranışları ve eleştirel düşünme becerilerini öğretmek.

BİT'i güvenli bir şekilde kullanmamıza bütün okul yaklaşımımız var ve bu emniyetli öğrenme ortamının yaratılması üç ana unsur içermektedir:

- etkili bir dizi teknolojik araç
- açık roller ve sorumluluklar içeren politikalar ve prosedürler
- öğrenciler, personel ve ebeveynler için kapsamlı bir e-güvenlik programı.

1.Amaç / Gerekçe

Yeni teknolojiler, hem okullarda hem de okul dışındaki hayatlarındaki günümüz toplumundaki çocukların ve genç insanların hayatları için ayrılmaz bir unsur haline geldi.

İnternet ve diğer dijital ve bilgi teknolojileri, herkes için yeni fırsatlar yaratan güçlü araçlardır. Elektronik iletişim, öğretmenlerin ve öğrencilerin birbirlerinden öğrenmesine yardımcı olur. Bu teknolojiler etkili bir öğrenmeyi teşvik etmek için tartışmayı teşvik edebilir, yaratıcılığı teşvik edebilir ve içeriğin farkındalığını artırabilir. Çocuklar ve gençler, her zaman güvenli internet erişimi hakkına sahip olmalıdır.

Çocukların ve gençlerin, çevrimiçi ve ilgili iletişim teknolojilerini uygun ve güvenli bir şekilde kullanabilmelerini sağlamak için gerekli şart, okullarda çalışanların hepsinin bağlı olduğu daha geniş bakım görevinin bir parçası olarak ele alınmaktadır. Okulun Çevrimiçi Güvenlik Politikası ve prosedürleri, güvenli ve uygun kullanımı sağlamak için yardımcı olacaktır. Böyle bir stratejinin geliştirilmesi ve uygulanması, çocuğun ana öğretmen ve valilerden üst düzey liderlere ve sınıf öğretmenlerine, destek personeline, velilere, topluluğun üyelerine ve öğrencilerin kendilerine yaptığı eğitimde tüm paydaşları içine alacaktır.

Bu heyecan verici ve yenilikçi araçların okulda ve evde kullanımı, eğitim standartlarını yükseltti ve öğrencinin başarısını artırdığı gösterildi. Bununla birlikte, bu yeni teknolojilerin kullanımı, gençleri okulun içinde ve dışında risk altına sokabilir.

Karşılaşılabilecekleri bazı tehlikeler şunlardır:

- Yasa dışı, zararlı veya uygunsuz görüntülere veya diğer içeriğe erişim;
- Kişisel bilgilerin yetkisiz olarak erişilmesi / kaybedilmesi / paylaşılması;
- İnternette temas kurdukları kişiler tarafından tımar edilmeye maruz kalma riski;
- Radikalleşmeyi teşvik etmek ve teşvik etmek için aşırılık yanlıları tarafından hedef alınma riski;
- Çocukların cinsel istismarı ile uğraşanlar tarafından hedef alınma riski;
- Kişisel fotoğrafların bireyin izni veya bilgisi olmaksızın paylaşımı / dağıtımı;
- Yanlışlar da dahil olmak üzere, uygunsuz iletişim / başkalarıyla iletişim;
- Siber zorbalık;
- Uygun olmayan video / internet oyunlarına erişim;
- İnternetteki bilgilerin kalitesini, doğruluğunu ve önemini değerlendirmede yetersizlik;
- İntihal ve telif hakkı ihlalleri;
- Müzik veya video dosyalarının yasadışı indirilmesi;
- Genç kişinin sosyal ve duygusal gelişimini ve öğrenimini etkileyebilecek aşırı kullanma potansiyeli.

Bu risklerin çoğu çevrimdışı dünyadaki durumları yansıtır ve bu Çevrimiçi Güvenlik Politikası ve prosedürlerinin, Kapsamlı Güvenlik

Koruma Bildirimi, Çocuk Koruma, Veri Koruma ve Tüm Okul Davranışı gibi diğer okul politikaları ile birlikte kullanılması önemlidir.

öğrencilerin maruz kalabilecekleri risklere karşı direncini arttırmak için gerekli önlemleri almak, böylece bu risklerle yüzleşmek ve bunlarla başa çıkma konusunda güven ve becerilere sahip olmak.

Okul, bu riskleri yönetmek ve azaltmak için makul olarak beklenebilecek her şeyi yaptıklarından emin olmak için gerekli önlemleri sağladığını göstermelidir. İnternet ve diğer iletişim teknolojilerini eğitime kullanırken, çevrimiçi güvenlik politikası ve izleyen süreçler, gençlerin (ve velilerinin) sorumlu kullanıcı olmalarına ve güvenli kalmalarına yardımcı olmak için daha geniş eğitim konularına değinirken bunu nasıl yapmayı planladığımızı açıklıyor , kişisel ve rekreasyonel kullanım.

E-Guvenlik & Okul Vizyonu

Inonu İlkokulunda, e-Guvenlik in, potansiyel zarar azaltmak için her türlü okul tedbirleri alınırken teknolojiyi güvenli, saygılı ve sorumlu bir şekilde kullanmanın sağladığı faydaları desteklemek olduğuna inanılmaktadır.

Etkili bir e-Guvenlik politikasının uygulanmasıyla koruma önlemleri belirlemeye ve okul topluluğunun tüm üyelerine riskleri dikkatle yönetme becerileri ile donatmaya çalışıyoruz. Öğrencilerimizin bilgi, iletişim teknolojileri (ICT) sorumluluk sahibi, yetkin, kendine güvenen ve yaratıcı kullanıcıları olmasını isteriz.

1.2. e-Güvenlik Politikasının Yürürlüğe Konulması ve Gözden Geçirilmesi

Turn ayarlar için uygun

1.1. Olası ifadeler:

Belirlenmiş Koruma Gücü (DSL: MEB internet Hattı)

Yönetim Organinin e-Güvenlik (e-Güvenlik) Uygulaması

F.YILDIZ # , ' '

Müdür Yardımcısı

Bay Öğretmen / Müdür tarafından onaylanan politika: E-Güvenlik Okul Politikası

Y.İPEK Tarih: 10.10.2022

Yönetim Organinin tarafından onaylanan politika: E-Güvenlik Okul Politikası

Sir sonraki politika incelemesinin tarihi 10.10.2023

- * Okçu Musa İlkokulu çevrimiçi güvenlik politikası, personel, öğrenci ve ebeveyn / bakıcıları içeren ve gerektiğinde uzman tavsiyesi ve girişi bulunan okul tarafından yazılmıştır.
- * Politika, Liderlik / Yönetim Ekibi ve Yönetim Organı tarafından onaylanmış ve kabul edilmiştir (ayar türüne uygun olarak değişiklik yapma).
- * Okul, Liderlik Takımı'nın uygun bir üyesi ve çevrimiçi güvenlik sorumlusu olarak Atanmış Koruma Gücü (adını) tayin etmiştir.
- * Okul, çevrimiçi güvenliğin (e-Güvenlik) sorumluluğunu üstlenmek üzere Yönetim Kurulunun bir üyesi olarak Adem ÖZÇELİK , görevlendirilmiştir.
- * Çevrimiçi güvenlik (e-Güvenlik) Politikası ve uygulanması, okul / ortam tarafından en az yılda bir kez veya gerekirse daha erken gözden geçirilecektir.

* 1.3 Toplum için temel sorumluluklar

* Tüm ayarlar için uygun

* 1.3.1 Okulun / ortam yönetiminin ve liderlik ekibinin temel sorumlulukları şunlardır:

- * * Okul toplumu genelinde uygun destek ve istişare ile ulusal ve yerel tavsiyelere uygun olarak tüm paydaşlara çevrimiçi güvenlik vizyonu ve kültürü geliştirmek, sahiplenmek ve tanıtmak.
- * * Çevrimiçi güvenliğin tüm topluluk tarafından korunan bir sorun olarak görülmesini ve güçlü bir çevrimiçi güvenlik kültürünün proaktif olarak geliştirilmesini sağlamak.

- * * Çevrimiçi Güvenlik rollerini ve sorumluluklarını yerine getirmek için yeterli zaman ve kaynağa sahip olmalarını sağlayarak Belirlenen Koruma Yönlendirmesini (DSL) desteklemek.
- * * Dahil olmak üzere çevrimiçi güvenlik ile ilgili uygun ve güncel politikalar ve prosedürler sağlanması Uygun profesyonel davranış ve teknolojinin kullanımını kapsayan Kabul Edilebilir Kullanım Politikası.
- * * Çocukların gerekli eğitim materyallerine erişebilmelerini sağlarken, okul topluluğunun ihtiyaçlarını karşılayan uygunsuz içeriği korumak için uygun ve uygun filtreleme ve izleme sistemlerinin mevcut olmasını sağlamak.

- * * Okul / ayar sistemleri ve ađlarının gvenliđini ve gvenliđini izlemede teknik personel ile birlikte alıřmak ve desteklemek ve okul / ayar ađ sisteminin aktif olarak izlenmesini sađlamak.
- * * Personelin tm yelerinin evrimii gvenlik rolleri ve sorumlulukları ile ilgili dzenli, gncel ve uygun eđitim almasını sađlamak ve gvenli uygun iletiřim hakkında rehberlik sađlamak.
- * * evrimii gvenliđin, tm ođrencilerin evrimii gvenliđi ve ilgili riskleri ve gvenli davranıřları yařlarına uygun bir anlayıř geliřtirmelerine olanak tanıyan, ilerlemeci bir btn okul / ortam mfredatına yerleřtirilmesini sađlamak.
- * * evrimii gvenlik olaylarından haberdar olmak ve harici ajansların ve destekleyicilerin uygun řekilde iletiřim kurmasını sađlamak.
- * * evrimii koruma kayıtlarını almak ve dzenli olarak gzden geirmek ve bunları gelecekteki uygulamaları bilgilendirmek ve řekillendirmek iin kullanmak.
- * * Okulun / ortamın i, yerel ve ulusal destek dahil olmak zere evrimii gvenlik endiřeleriyle ilgili olarak eriřmesi iin sađlam raporlama kanalları olduđundan emin olmak.
- * * Cihazların gvenli ve sorumlu kullanımının sađlanması dahil, teknolojinin gvenli kullanımı ile ilgili uygun risk deđerlendirmelerinin yapıldıđından emin olun.
- * * Ynetim organının bir yesinin evrimii gvenliđin desteklenmesi iin ana sorumluluk olarak tanımlanmasını sađlamak.
- * • Geliřmekte olan gl yanları ve alanları belirlemek iin mevcut evrimii gvenlik uygulamalarını denetlemek ve deđerlendirmek.

- * • Belirlenen Koruma Yönlendirmesi'nin (DSL) çevrimiçi güvenlik sorumlusu ile çalışmasını sağlamak.

1.3.2 Atanmış Koruma Amaçlı Kurşunun ana sorumlulukları şunlardır:

- * Tüm çevrimiçi korunma konularında bir irtibat noktası olarak hareket etmek ve uygun şekilde diğer personel ve diğer kurumlarla irtibat kurmak.
- * Çevrimiçi güvenlik ile ilgili güncel araştırma, mevzuat ve trendler ile güncel tutmak.
- * Olumlu çevrimiçi davranışı teşvik etmek için yerel ve ulusal etkinliklere katılımın koordine edilmesi, ör. Daha Güvenli İnternet Günü.

* Çevrimiçi güvenliğin, çeşitli kanallar ve yaklaşımlar aracılığıyla ebeveynlere ve bakıcılara ve daha geniş topluluklara tanıtılmasının sağlanması.

* Uygulamanın güncel mevzuata uygun olmasını sağlamak için veri koruma ve veri güvenliği için okul / ayar kurumu ile çalışın.

* Kayıt yapılarını ve mekanizmalarını koruyan okulların bir parçası olarak alınan çevrimiçi güvenlik kaygılarının / olaylarının ve eylemlerinin kaydını tutmak.

* Boşlukları / eğilimleri tanımlamak için okulu / ayarları çevrimiçi güvenlik olaylarını izleyin ve bu verileri, ihtiyacı yansıtacak şekilde okul / ayarlar eğitim yanıtını güncellemek için kullanın.

* Çevrimiçi güvenlik kaygıları ve yerel veriler / rakamlar konusunda okul yönetim ekibine, Yönetim Organına ve diğer kurumlara rapor vermek.

* Yerel ve ulusal kurumlarla uygun şekilde ilişki kurmak.

* Çevrimiçi güvenlik politikalarını, Kabul Edilebilir Kullanım Politikalarını (AUPs) ve ilgili diğer politikaları düzenli olarak (en az yılda bir kez) paydaş girdisi ile gözden geçirmek ve güncellemek için okul / ayar liderliği ve yönetimi ile çalışmak.

* Çevrimiçi güvenliğin diğer uygun okul politikaları ve prosedürleriyle entegre edilmesini sağlamak.

• Tüm paydaş gruplarından girdi içeren bir çevrimiçi güvenlik ekibi /

grubunun liderliğinde.

- Çevrimiçi güvenlik sorumlusu olan okul müdürü ile düzenli olarak görüşülecek.

1.3.3 Tüm personel üyeleri için temel sorumluluklar şunlardır:

- * Çevrimiçi güvenlik politikalarının geliştirilmesine katkıda bulunmak.
- * Okul Kabul Edilebilir Kullanım Politikalarını (AUPs) okumak ve onlara bağlı kalmak.
- * Okul / ayar sistemleri ve verilerin güvenliği için sorumluluk almak.
- * Bir dizi farklı çevrimiçi güvenlik sorununa ve onların bakımındaki çocuklarla nasıl ilişki kurabileceğine dair farkındalığa sahip olmak.
- * Yeni ve gelişmekte olan teknolojileri kullanırken iyi uygulamaların modellenmesi
- * Mümkün olan yerlerde çevrimiçi güvenlik eğitimini müfredata ulaştırmak.

İlgili kişileri tespit etmek ve okul koruma politikalarını ve prosedürlerini takip ederek uygun önlemleri almak.

* İnternette ve dışarıdan çevrimiçi güvenlik sorunlarını ne zaman ve nasıl arttıracığını bilmek.

* Çevrimiçi güvenlik sorunları için dahili ve harici olarak uygun desteklere imza atmak.

* Hem kendi içinde hem de dışında kendi kişisel teknoloji kullanımında profesyonel bir davranış düzeyini sürdürmek.

• Olumlu öğrenme fırsatlarına vurgu yapmak.

• Bu alanda mesleki gelişim için kişisel sorumluluk almak.

1.3.4 Yukarıdakilere ek olarak, teknik ortamı yöneten personel için temel sorumluluklar şunlardır:

* Öğrenim fırsatlarının hala en üst düzeye çıkarılmasını sağlarken güvenli çevrimiçi uygulamaları destekleyen güvenli ve güvenli bir teknik altyapı sağlamak.

* Liderlik ve yönetim ekibiyle ortaklaşa sistem ve verilerin güvenli bir şekilde güvenliğini sağlamak için sorumluluk almak.

* Okuldaki cihazlarda tutulan kişisel ve hassas bilgileri korumak için uygun erişim kontrolleri ve şifrelemenin yapıldığından emin olmak.

* Okullar için filtreleme politikasının düzenli olarak uygulanması ve güncellenmesinin sağlanması ve uygulanmasının sorumluluğunun DSL ile paylaşılması.

* Okulun / ayarın ağının kullanımının düzenli olarak izlenmesini ve DSL'e herhangi bir kasıtlı veya tesadüfi yanlış kullanım bildirilmesini sağlamak.

* Herhangi bir ihlal veya endişeyi DSLand liderlik

ekibine bildirin ve birlikte kaydedildiğinden ve tavsiye edildiği şekilde uygun önlemlerin alındığından emin olunacak

** Teknik altyapının güvenliği ve güvenliği ile ilgili olarak ilgili mevzuatın anlaşılmasını geliştirmek.*

** Herhangi bir ihlali rapor etmek ve teknik altyapı konularında uygun olan yerel makamlarla (veya diğer yerel veya ulusal kurumlarla) irtibat kurmak.*

** DSL ve liderlik ekibine, özellikle uygun çevrimiçi güvenlik politikaları ve prosedürlerinin geliştirilmesi ve uygulanmasında teknik destek ve bakış açısı sağlamak.*

• Okulun BİT altyapısının / sisteminin güvenli ve kötü amaçlı veya kötü niyetli saldırılara açık olmaması.

- Tüm ayar makineleri ve taşınabilir aygıtlarda uygun anti-virüs yazılımı ve sistem güncellemelerinin kurulup sürdürülmesini sağlamak.
- Uygun olan güçlü şifrelerin, ancak en genç kullanıcılar için uygulandığından ve uygulandığından emin olun.

1.3.5 Çocukların ve gençlerin temel sorumlulukları şunlardır:

- * Çevrimiçi güvenlik politikalarının geliştirilmesine katkıda bulunmak.
- * Okulu okumak / Kabul Edilebilir Kullanım Politikalarını (AUPs) okumak ve onlara bağlı kalmak.
- * Başkalarının hem çevrimiçi hem de çevrimdışı duygularına saygı duymak.
- * Bir şeyler ters giderse, güvenilen bir yetişkinden yardım almak ve çevrimiçi güvenlik sorunları yaşayabilen diğer kişileri desteklemek.

Kendi yaşlarına, yeteneklerine ve güvenlik açıklarına uygun bir düzeyde:

- * Kendilerini ve başkalarını çevrimiçi ortamda güvende tutmak için sorumluluk almak.
- * Yeni ve gelişmekte olan teknolojilerin ortaya çıkardığı fırsatlar ve riskler ile ilgili olarak kendi farkındalık ve öğrenme sorumluluğunu üstlenmek.
- * Belirli bir teknolojiyi kullanmanın kişisel risklerini değerlendirmek ve

bu riskleri sınırlamak için güvenli ve sorumlu davranmak.

1.3.6 Ebeveynlerin ve bakıcıların temel sorumlulukları şunlardır:

* Okumayı / Kabul Edilebilir Kullanım Politikalarını okuyup okumaya, çocuklarını kendilerine bağlı kalmaya teşvik etmeye ve uygun durumlarda kendilerine bağlı kalmaya.

* Çocuklarıyla çevrimiçi güvenlik sorunlarını tartışmak, çevrimiçi güvenlik yaklaşımlarında okulu desteklemek ve evde güvenli çevrimiçi davranışları güçlendirmek.

* Rol modelleme teknolojinin ve sosyal medyanın güvenli ve uygun kullanımı.

* Çocuğunun çevrimiçi zarar görme riski taşıdığını belirten davranış değişiklikleri.

* Onlar veya çocuklarıyla karşılaşırsa okuldan veya diğer uygun kurumlardan yardım ve destek istemek

* Çevrimiçi sorunlar veya endişeler.

• Okulun geliştirilmesine / çevrimiçi güvenlik politikalarının belirlenmesine katkıda bulunmak.

• Öğrenme platformları ve diğer ağ kaynakları gibi okul sistemlerini güvenli ve uygun bir şekilde kullanma.

• Yeni ve gelişmekte olan teknolojilerin ortaya çıkardığı fırsatlar ve risklerle ilgili olarak kendi farkındalıklarını ve öğrenmelerini sağlamak.

2.Çevrimiçi İletişim ve Teknolojinin Daha Güvenli Kullanımı

2.1 Okul / ayar web sitesini

yönetmek Bir web sitesi

barındıran ayarlarla ilgili

Olası ifadeler:

* Web sitesindeki iletişim bilgileri okul / ayar adresi, e-posta ve telefon numarası olacaktır. Personel veya öğrencilerin kişisel bilgileri yayınlanmayacaktır.

* Okul müdürü yayınlanan çevrimiçi içerik için genel içerik sorumluluğu alacak ve bilgilerin doğru ve uygun olmasını sağlayacaktır.

* Web sitesi, fikri mülkiyet hakları, gizlilik politikaları ve telif hakkıyla ilgili erişilebilirliğe saygıyı içeren yayınlar için okulun kılavuz ilkelerine uyacaktır.

• E-posta adresleri spam olarak toplanmamak için ('@' yerine 'AT')

ile) kaçınmak için çevrimiçi olarak dikkatli bir şekilde yayınlanacaktır.

- Öğrenciler çalışma izni veya ebeveynleri / bakıcıları ile yayınlanacaktır.
- Okul web sitesinin yönetici hesabı uygun bir şekilde güçlü bir parola ile korunacaktır.
- Okul, çevrimiçi güvenlik dahil olmak üzere, toplumun üyeleri için okulun web sitesinde koruma hakkında bilgi yayınlayacaktır.

2.2 Görüntüleri ve videoları çevrimiçi

yayınlama Olası ifadeler:

- * Okul / ortam, çevrimiçi paylaşılan tüm görsellerin ve videoların, okul imajı kullanım politikasına uygun olarak kullanılmasını sağlayacaktır.
- * Okul / ortam, görüntülerin ve videoların tüm kullanımının, veri güvenliği, Kabul Edilebilir Kullanım Politikaları, Davranış Kuralları, sosyal medya, kişisel cihazların ve cep telefonlarının kullanımı gibi diğer politika ve prosedürlere uygun olarak gerçekleştirilmesini sağlayacaktır.

* Görüntü politikasına uygun olarak, ebeveynlerin veya bakıcıların yazılı izni her zaman, öğrencilerin görüntüleri / videoları elektronik olarak yayınlanmadan elde edilecektir.

2.4 Eğitim amaçlı resmi video konferans ve webcam kullanımı
Görüntülü konferans ve web kamerası kullanan tüm ayarlar için önemlidir

2.4 Olası ifadeler:

* Okul video konferansın çok çeşitli öğrenme faydaları ile zorlayıcı bir etkinlik olduğunu kabul eder. Hazırlık ve değerlendirme tüm faaliyet için gereklidir.

* Tüm video konferans ekipmanı kullanılmadığında ve uygun olduğunda otomatik cevap olarak ayarlanmadığında kapatılacaktır.

- Harici IP adresleri diğer sitelere sunulmayacaktır.
- Video konferans iletişim bilgileri yayınlanmayacaktır.
- Video konferans ekipmanı güvenli bir şekilde saklanacak ve gerektiğinde kullanılmadığında kilitlenecektir.
- Okul video konferans ekipmanı izinsiz olarak okul tesislerinden çıkarılmayacaktır.
- Personel harici video konferans fırsatlarının ve / veya araçlarının uygun bir şekilde değerlendirildiğinden ve olaylara erişmek için kullanılan hesapların ve sistemlerin uygun şekilde güvenli ve güvenli olmasını sağlayacaktır.

Kullanıcılar

* Öğrenciler bir video konferans görüşmesi veya mesajı yapmadan veya cevaplamadan önce bir öğretmenden izin isteyeceklerdir.

* Video konferans, öğrencilerin yaş ve yetenekleri için uygun şekilde

denetlenecektir.

- * Video konferans etkinliklerine katılan çocuklardan önce veliler ve bakıcılar onayı alınacaktır.
- * Video konferans, güçlü bir risk değerlendirmesinin ardından resmi ve onaylanmış iletişim kanalları aracılığıyla gerçekleştirilecektir.
- Video konferans yönetimi alanlarına veya uzaktan kontrol sayfalarına yalnızca kilit yöneticilere erişim verilecektir.
- Eğitsel video konferans hizmetleri için benzersiz oturum açma ve şifre bilgileri sadece personel üyelerine verilir ve güvende tutulur.

içerik

- Bir video konferans dersi kaydederken, tüm siteler ve katılımcılar tarafından yazılı izin verilecektir. Kaydın nedeni verilmeli ve konferans başlangıcında video konferansın kaydı tüm taraflara açık olmalıdır. Kaydedilen materyal güvenli bir şekilde saklanacaktır.

- Üçüncü taraf materyalleri dahil edilecekse, okul üçüncü şahıs fikri mülkiyet haklarını ihlal etmekten kaçınmak için kaydın kabul edilebilir olduğunu kontrol edecektir.
- Okul, video konferansa katılmadan önce diğer konferans katılımcılarıyla diyalog kuracaktır. Okul dışı bir siteyse, okul, sınıfa uygun materyalleri teslim ettiklerini kontrol edecektir.

2.5 İnternetin ve ilgili cihazların uygun ve

güvenli sınıf içi kullanımı Çocuklar için internet

erişimi sağlayan tüm ayarlar için uygun

2.5 Olası ifadeler:

- * * İnternet kullanımı, eğitimsel erişimin önemli bir özelliğidir ve tüm çocukların yaşları kabul edip, bütünlük bir okul müfredatının bir parçası olarak endişelere yanıt vermek için stratejiler geliştirmelerini desteklemek ve desteklemek için uygun eğitime sahip olmaları gerekir.
- * * Okulun / ortamın internet erişimi eğitimi geliştirmek ve genişletmek için tasarlanacaktır.
- * * İnternete erişim seviyeleri, müfredat gereksinimlerini ve öğrencilerin yaşını ve yeteneklerini yansıtacak şekilde gözden geçirilecektir.
- * * Tüm çalışanlar, çocukları korumak için tek başına filtrelemeye dayanamayacaklarını ve güvenli ve sorumlu kullanımla ilgili gözetim, sınıf yönetimi ve eğitimin gerekli olduğunu biliyorlar.

- * * Öğrencilerin gözetimi yaşlarına ve yeteneklerine uygun olacaktır.
- * Genç öğrencilerin İnternet'e erişimleri, yetişkinlerin gözetiminde, öğrencilerin yaşları ve yetenekleri için planlanan öğrenme çıktılarını destekleyen belirli ve onaylanmış çevrimiçi materyallere doğrudan denetimli erişim ile olacaktır.
- * 5-10 yaş arası öğrenciler denetlenecek. Öğrenciler yaş uygun arama motorlarını kullanacak ve çevrimiçi araçlar ve çevrimiçi aktiviteler gerektiğinde öğretmene yönelik olacaktır. Çocuklar, öğrencilerin yaşları ve yetenekleri için planlanan öğrenme çıktılarını destekleyen çevrimiçi materyallere ve kaynaklara yönlendirilecektir.
- * Teknolojiyi kullanırken yetenek ve anlayışlarına göre öğrenciler uygun şekilde denetlenecektir.

- * Tüm okul cihazları, Kabul Edilebilir Kullanım Politikasına ve uygun güvenlik ve güvenlik önlemlerine uygun olarak kullanılacaktır.
- * Personel üyeleri web sitelerinde kullanmadan önce web sitelerini, araçlarını ve uygulamaları her zaman değerlendirecek veya evde kullanmayı önereceklerdir.
- * Öğrencilerin bilgi konumu, geri kazanımı ve değerlendirilmesi becerileri de dahil olmak üzere, araştırmada İnternetin etkin kullanımı konusunda eğitileceklerdir.
- * Okul, internet türevi materyallerin personel ve öğrenciler tarafından kullanılmasının telif hakkı yasasına uyduğunu ve bilgi kaynağının kabul edildiğini garanti edecektir.
- Öğrencilere, okudukları materyalleri eleştirel olarak bilmeleri ve doğruluğunu kabul etmeden önce bilgiyi nasıl doğrulayacakları gösterilecektir.
- Çevrimiçi materyallerin değerlendirilmesi, her konuda öğretme ve öğrenmenin bir parçasıdır ve müfredat genelinde bir okul / ortam şartı olarak görülecektir.
- Okul, öğrencilerin ve çalışanların güvenli ve güvenli bir ortamda iletişim kurmasını ve işbirliği yapmasını sağlamak için interneti kullanacaktır.

Sosyal Medya Politikası

3.1.Genel sosyal medya

kullanımı Tüm ayarlar için

uygun

3.1. Olası ifadeler:

* Sosyal medyanın güvenli ve sorumlu kullanımıyla ilgili beklentiler, hem okul / ortam hem de daha geniş toplulukları, hem çevrimiçi hem de çevrimdışı olarak korumak için Okçu Musa İlkokulu topluluğunun tüm üyeleri için geçerli olacak ve var olacaktır. Sosyal medya örnekleri arasında bloglar, wiki'ler, sosyal ağ siteleri, forumlar, bülten panoları, çok oyunculu çevrimiçi oyunlar, uygulamalar, video / fotoğraf paylaşım siteleri, sohbet odaları, anlık mesajlaşma ve daha pek çok şey bulunabilir.

* Okçu Musa İlkokulu topluluğunun tüm üyeleri, sosyal medyaya her zaman olumlu, güvenli ve sorumlu bir şekilde katılmaya teşvik edilecektir.

* Sosyal medyanın güvenli ve sorumlu kullanımıyla ilgili bilgiler, açık bir şekilde ve düzenli olarak Okçu Musa İlkokulu topluluğu üyelerine iletilecektir.

* Okçu Musa İlkokulu topluluğunun tüm üyelerine, herhangi bir sosyal medya hizmetinde, özellikle de tehdit edici, incitici veya başkalarına karşı iftira niteliğinde olabilecek, özel ve ayrıntılı özel düşünceler, endişeler, resimler veya mesajlar yayınlamaması tavsiye edilir.

* Okul / ortam, sitede ve okul tarafından sağlanan cihaz ve sistemleri kullanırken, öğrenci ve personelin sosyal medya ve sosyal ağ sitelerine erişimini kontrol edecektir .

* Okul saatleri içinde kişisel kullanım için sosyal ağ uygulamalarının kullanılması / sunulması zorunlu değildir . Bu, öğrencilerin yaşına / yeteneklerine ve personel erişimine karar verildiğinde farklılık gösterecektir.

* Okul / çalışma saatlerinde veya okul / ayar cihazları kullanırken sosyal medyanın uygunsuz veya aşırı kullanımı disiplin cezası veya yasal işlem ve / veya internet tesislerinin kaldırılmasıyla sonuçlanabilir.

* Sosyal medya sitelerinde Okçu Musa İlkokulu topluluğunun herhangi bir üyesinin çevrimiçi davranışına ilişkin kaygılar liderlik ekibine bildirilmeli ve anti-zorbalık, personele yönelik iddialar, davranış ve korunma gibi politikalara uygun olarak yönetilmelidir. /Çocuk koruma.

* Okul belirleme politikasının ihlalleri cezai, disiplin cezası veya sivil eylemlere yol açabilir ve bu, ilgili kişilerin yaşına ve işlenen yanlışın koşullarına bağlı olacaktır. Alınan önlemler, anti-zorbalık, personele yönelik iddialar, davranış ve korunma çocuk koruma gibi ilgili politikalara uygun olacaktır.

3.2. Sosyal medyanın resmi kullanımı

Sosyal medyayı resmi olarak bir iletişim kanalı olarak kullanan tüm ayarlar için geçerlidir.

3.2 Olası ifadeler:

* Okçu Musa İlkokulu resmi sosyal medya kanalları şunlardır:

Liste detayları ör. Okul Web Sitesi,Eba bağlantısı.

* Sosyal medya sitelerinin okul ortam tarafından resmi olarak kullanılması, yalnızca belirli bir hedefe yönelik sonuçlarla net

eđitim veya toplum katılım hedefleriyle gerekleřtirilecektir. ebeveyn katılımını arttırmak.

* İletişim araçları olarak sosyal medya sitelerinin resmi kullanımı risk deęerlendirmesine tabi olacak ve m¼d¼r / y¼netici tarafından resmi olarak onaylanacaktır (ortama uygun olarak).

* Resmi okul / sosyal medya kanallarını belirleme, farklı ve özel sosyal medya sitesi olarak kurulacak veya eđitim veya niřan alma amacıyla hesaplanacaktır.

* Personel resmi onaylı sosyal medya kanallarına kaydolmak ve y¼netmek iin okul / ayar e-posta adreslerini kullanacaktır.

* Resmi sosyal medya kanallarını y¼neten personelin ¼yeleri, gerekli davranıřların ve kullanım beklentilerinin farkında olduklarından ve sitelerin g¼venli, sorumlu ve yerel ve ulusal rehberlięe uygun olarak kullanılmalarını saęlamak iin belirli bir Kabul Edilebilir Kullanım Politikasını (AUP) imzalayacaklardır. ve mevzuat.

* Resmi sosyal medya platformlarındaki t¼m iletişim aık, řeffaf ve incelemeye aık olacaktır.

* Resmi sosyal medya siteleri ile ilgili herhangi bir çevrimiçi yayın, 1998 tarihli İnsan Hakları Yasası'nın sağladığı gizlilik hakkı ya da özel bilgileri korumaya yönelik benzer bir görev olan ve Gizlilikle ilgili herhangi bir ortak kanunu ihlal etmeyecek olan Veri Koruma Yasası 1998 de dahil olmak üzere yasal gerekliliklere uygun olacaktır. telif hakkı vb

* Resmi sosyal medya kullanımı, anti-zorbalık ve çocuk koruma dahil olmak üzere mevcut politikalara uygun olacaktır.

* Resimlerin veya videoların görüntüleri yalnızca resmi sosyal medya sitelerinde / kanallarında görüntü kullanım politikasına uygun olarak paylaşılacaktır.

* Sosyal medya kanallarının güvenli ve sorumlu kullanımıyla ilgili bilgiler, topluluğun tüm üyelerine açık ve düzenli olarak iletilecektir.

* Resmi sosyal medya siteleri, bloglar veya wiki'ler uygun bir şekilde korunacaktır (örn., Şifre korumalı) ve mümkün olan yerlerde / uygun olduğunda, okul / ayar web sitesinden işletilecek ve / veya bağlanacaktır ve Liderlik Ekibinin yazılı onayı ile gerçekleştirilecektir.

* Liderlik personeli, personelin olmaması gibi acil durumlarda sosyal medya kanalları için hesap bilgilerinin ve ilgili detayların farkında olmalıdır.

* Ebeveynler / Bakıcılar ve öğrenciler resmi sosyal medya kullanımından, güvenli kullanım beklentileri ve toplumu korumak için alınan önlemlerden haberdar edilecektir.

• Okul / ortam adına kamusal iletişim, mümkün olduğunda, en az bir başka meslektaş tarafından okunup kabul edilecektir.

• Resmi sosyal medya kanalları okul / ayar web sitesine ve / veya

Kabul Edilebilir Kullanım Politikasına geri bağlantı sağlayacaktır.

- *hesabın resmi olduğunu gösterin.*

- *Okul / ortam, herhangi bir resmi sosyal medya kullanımının, sosyal medya kanallarını kullanamayan veya kullanamayan topluluk üyelerini hariç tutmamasını sağlayacaktır.*

3.3 Personelin sosyal medyayı kişisel

kullanımı Tüm ayarlar için uygun

3.3 Olası ifadeler:

** Sosyal ağların, sosyal medyanın ve kişisel yayın sitelerinin güvenli ve sorumlu kullanımı, personelin tüm personeli ile tartışılacak ve düzenli personel eğitim fırsatları ile yeniden gözden geçirilecek ve iletilecektir.*

- * Güvenli ve profesyonel davranışlar, personelin (gönüllüler dahil) tüm üyeleri için Kabul Edilebilir Kullanım Politikasının / okulunun bir parçası olarak özetlenecektir.
- * Tüm personel üyelerine, herhangi bir kişisel sosyal medya siteleri, uygulamalar veya profiller aracılığıyla mevcut veya geçmiş çocuk / öğrenciler veya şimdiki veya geçmiş öğrencilerin aile fertleri ile iletişim kurmaları veya “arkadaş” olarak eklememeleri tavsiye edilir. Bunu tehlikeye atabilecek önceden var olan herhangi bir ilişki veya istisna, Atanmış Koruma Gücü ve / veya ana öğretmen ile tartışılacaktır.
- * Öğrencilerle devam eden temaslar okuldan ayrıldıktan sonra gerekliyse, personel üyelerinin mevcut mezun ağlarını kullanması veya resmi okulun sağladığı iletişim araçlarını kullanması beklenir.
- * Okulla ilgili çalışanlar ve okul topluluğu üyeleri arasındaki tüm iletişim, resmi onaylı iletişim kanalları aracılığıyla yapılacaktır (resmi ayar olarak e-posta adresi veya telefon numaraları gibi)
- * Personel, öğrenci veya velilerle iletişim kurmak için kişisel sosyal medya hesaplarını kullanmaz veya herhangi bir iletişimin kabul edilmesini gerektirmez.
- * Kişisel sosyal medya hesaplarından öğrenilen öğrencilerden / velilerden gelen her türlü iletişim, koruyucu aday olarak belirlenen okullara bildirilecektir.
- * Öğrencilerin fotoğraf ve kişisel bilgileri, öğrenciler ve aile üyeleri, meslektaşları vb. Dahil olmak üzere, istihdamlarının bir parçası olarak erişebilecekleri bilgi ve içerik, kişisel sosyal medya sitelerinde paylaşılmayacak veya tartışılmayacaktır.
- * Sosyal medya sitelerini kullanırken personelin tüm üyelerinin kendilerini ve gizliliklerini korumaları şiddetle tavsiye edilir. Bu, konum paylaşım hizmetlerinin farkında olmak, kişisel sitelerinin gizlilik

seviyelerini olabildiğince sıkı bir şekilde ayarlamak, sosyal ağ sitelerinde halka açık girişleri kapatmak, kullandıktan sonra hesaplarını kapatmak ve şifrelerin güvenli ve gizli kalmasını içerecektir.

* Tüm personel üyeleri, çevrimiçi olarak paylaştıkları ve yayınladıkları metin ve görseller de dahil olmak üzere bilgileri dikkatlice değerlendirmeye ve sosyal medya kullanımlarının mesleki rolleri ile uyumlu olmasını ve okul politikalarına (güvenlik, gizlilik, veri) uygun olmasını sağlamaya teşvik edilir. koruma vb.) ve daha geniş profesyonel ve yasal çerçeve.

* Çalışanların, paylaştıkları ve çevrimiçi yayınladıkları içeriği yönetmeleri ve kontrol etmeleri teşvik edilecektir. Personele personel eğitimi yoluyla ve düzenli olarak uygun rehberlik ve kaynaklar paylaşarak danışmanlık sağlanacaktır.

* Personel üyeleri, e-postalar veya sosyal ağ siteleri de dahil olmak üzere okul / ortamdaki rolleriyle çatışan herhangi bir bilgi ve iletişim teknolojisi yoluyla paylaşılan veya yayınlanan herhangi bir içeriğin derhal dikkate alınması halinde Liderlik / Yönetim Ekibine bildirimde bulunacaklardır.

- Personel üyeleri, kendilerini kişisel sosyal ağ hesaplarında Okçu Musa ilkokulu çalışanı olarak tanımlamamak için teşvik edilir. Bu, bu sitelerdeki bilgilerin okul / ortam ile bağlantılı olmasını ve ayrıca personelin ve daha geniş toplumun gizliliğini korumalarını önlemektir.
- Personel üyeleri, kişisel görüşlerini sosyal medyadaki okul / ortam olarak temsil etmemelerini sağlayacaktır.
- Kişisel sosyal medya hesaplarını kurmak için okul / ayar e-posta adresleri kullanılmayacaktır.
- Okul / ortam sosyal medya kanallarını takip eden / beğenen personelin, mümkün olan yerlerde profesyonel sınırların bulanıklaşmasından kaçınmak için özel profesyonel hesaplar kullanmaları tavsiye edilir.

3.3 Sosyal medyanın resmi

kullanımı Tüm ayarlar için

uygun

3.4 Olası ifadeler:

** Personel, çevrimiçi etkinliklere, okul / ortam çalışanı olarak kapasitelerinin bir parçası olarak katılıyorsa, her zaman profesyonel olmaları ve okul / ortam için büyükelçi olduklarının bilincinde olmaları istenir.*

** Sosyal medyayı resmi olarak görevlendiren personel resmi rollerini / pozisyonlarını açıklayacak, ancak her zaman okul / ortam adına konuşmamaları gerektiğini açıkça belirtecektir.*

** Resmi olarak sosyal medyayı kullanan personel, her zaman sorumlu,*

güvenilir, dürüst ve dürüst olacaktır ve yayınlanmakta olan bilgilerin nasıl algılanabileceğini veya paylaşılabilirliğini düşünecektir.

** Sosyal medyayı resmi olarak görevlendiren personel, işyerinde uyuşmazlıkları, hakaretleri, gizliliği, telif hakkı, veri koruma ve eşitlik yasaları dahil olmak üzere işyerindeki yasal çerçeveler çerçevesinde hareket edecektir.*

** Personel, herhangi bir resmi sosyal medya kanalında yayınlanan herhangi bir görüntünün uygun bir yazılı ebeveyn izni almasını sağlamalıdır.*

** Sosyal medyayı resmi olarak görevlendiren personel hesap verebilir ve bilgi verme, taahhütte bulunmama veya okul / ortam adına faaliyette bulunma yetkisine sahip olmadıkça sorumlu değildir.*

** Sosyal medyayı kullanan personel resmi olarak, online olarak yayınlanan eleştiri veya uygunsuz içerik gibi herhangi bir kaygının hat yöneticisini, Atanmış Koruma Görevini ve / veya baş öğretmeni / yöneticisini bilgilendirecektir.*

* Personel sosyal medya aracılığıyla çocuklarla veya ebeveynlerle / bakıcılarla doğrudan veya özel mesajlaşmaya girmeyecek ve resmi iletişim kanalları aracılığıyla iletişim kuracaktır.

* Sosyal medyayı kullanan personel resmi olarak okul / sosyal medya Kabul Edilebilir Kullanım Politikası'nı imzalayacaktır.

Sosyal medyayı kullanan öğrenciler

Tüm ortamlarla ilgili, ancak çocukların yaşına ve yeteneklerine göre adapte edilmesi gerekecektir.

3.5 Olası ifadeler:

* Sosyal medya sitelerinin güvenli ve sorumlu kullanımı, Kabul Edilebilir Kullanım Politikası'nın bir parçası olarak çocuklar ve ebeveynleri için ana hatlarıyla belirtilecektir.

* Sosyal medya sitelerinde kişisel yayınlar, öğrencilere eğitim amaçlı uygun olarak değerlendirilen ve onaylanan gömülü ve ilerici eğitim yaklaşımının yaşına uygun alanlarının bir parçası olarak öğrencilere öğretilecektir.

* Öğrencilere, kendilerini ve / veya yerlerini belirleyebilecek sosyal medya sitelerinde kişisel bilgilerin paylaşılma risklerini dikkate almaları önerilir. Örnekler arasında gerçek

/ tam isim, adres, cep telefonu veya sabit telefon numaraları, okula gidenler, Anında mesajlaşma iletişim bilgileri, e-posta adresleri, arkadaş / aile adları, özel ilgi alanları ve kulüpler vb.

* Öğrenciler, ebeveynleri / bakıcıları veya diğer sorumlu yetişkinlerin izni olmadan herhangi bir çevrimiçi arkadaşla buluşmamaları ve yalnızca mevcut oldukları zaman bilgilendirilmeleri tavsiye edilir.

** Öğrenciler sosyal medya sitelerinde uygun güvenlik konusunda bilgilendirilecek ve güvenli ve şifreler kullanmaya, bilinmeyen kişilere erişimi engellemeye ve istenmeyen iletişimlerin nasıl engellenip raporlanabileceğini öğrenmeye teşvik edilecektir.*

** Öğrenciler, yalnızca sosyal paylaşım sitelerinde bilinen arkadaşları onaylamaya ve davet etmeye ve profilleri özel / korumalı yaparak başkalarına erişimi engellemeye teşvik edilecektir.*

** Ebeveynlere resmi sosyal medya kullanımı hakkında bilgi verilecek ve gerektiğinde yazılı ebeveyn izni alınacaktır.*

* Öğrencileri içeren herhangi bir resmi sosyal medya etkinliği mümkün olan yerlerde okul tarafından yönetilecektir.

* Okul, birçok popüler sosyal medya sitesinin 13 yaşın altındaki çocuklar için olmadığını belirtmektedir, bu nedenle Okul, özellikle bu yaşın altındaki çocuklar için okul içinde hesap oluşturmayacaktır.

* Öğrencilerin hem evde hem de okulda sosyal ağ, sosyal medya ve kişisel yayıncılık sitelerini kullanmalarına ilişkin kaygılar, zorbalık karşıtı ve davranışlar da dahil olmak üzere mevcut okul politikalarına uygun olarak ele alınacaktır.

* Özellikle sosyal medya sitelerinin reşit olmayan kullanımı ile ilgili olarak, öğrencilerin hem evde hem de okulda sosyal ağ, sosyal medya ve kişisel yayın sitelerini kullanmalarına ilişkin kaygılar anne babalar / bakıcılar ile yükseltilecektir.

4. Kişisel Cihazların ve Cep

Telefonlarının Kullanımı Tüm ayarlar

için uygun

Tartışma:

4.1 Kişisel cihazlar ve cep telefonları ile ilgili mantık

4.1 Olası ifadeler:

* Cep telefonlarının ve çocuk, genç ve yetişkinler arasında bir dizi diğer kişisel cihazların yaygın bir şekilde sahiplenilmesi, tüm kullanıcıların Okçu Musa İlkokulu topluluklarının, cep telefonlarının ve kişisel cihazların sorumlu bir şekilde kullanılmasını sağlamak için gerekli adımları atmasını gerektirecektir.

** Genler ve yetiřkinler tarafından cep telefonları ve dięer kiřisel cihazların kullanımı, okul / ortam tarafından kararlařtırılacak ve kabul edilebilir Kullanım veya Cep Telefonu Politikası dahil olmak üzere uygun politikalarda ele alınacaktır.*

** Okçu Musa ilkokulu mobil teknolojiler aracılıęıyla kiřisel iletiřimin ocuklar, alıřanlar ve ebeveynler / bakıcılar iin gnlk yařamın kabul edilen bir parası olduęunu kabul eder, ancak bu tr teknolojilerin okullarda / ortamlarda gvenli ve uygun bir Őekilde kullanılmasını gerektirir.*

4.2 Kiřisel cihazların ve cep telefonlarının gvenli kullanımı iin beklentiler

4.2 Olası ifadeler:

* Kişisel cihazların ve cep telefonlarının tüm kullanımı yasalara ve diğer uygun okul politikalarına uygun olarak gerçekleştirilecektir (uygun şekilde liste).

* Sitede getirilen her türlü elektronik cihaz, kullanıcının sorumluluğundadır. Okul / ayar, bu tür eşyaların kaybolması, çalınması veya zarar görmesi için sorumluluk kabul etmez. Okul / ortam, bu tür cihazların neden olabileceği herhangi bir yan etki veya potansiyel için sorumluluk kabul etmez.

* Cep telefonları ve kişisel cihazların okul / şantiyede soyunma odaları, tuvaletler ve yüzme havuzları gibi belirli alanlarda kullanılmasına izin verilmez.

* Küfürlü veya uygunsuz mesajların veya içeriğin cep telefonları veya kişisel cihazlarla gönderilmesi, toplumun herhangi bir üyesi tarafından yasaklanmıştır ve herhangi bir ihlal, / disiplinine / davranış politikasının bir parçası olarak ele alınacaktır.

* Personel üyeleri, öğrencilerin veya ebeveynlerin / bakıcıların gerekli olduğu bir iş telefonu numarası ve e-posta adresi ile verilecektir.

* Okçu Musa ilkokulu topluluğunun tüm üyelerine cep telefonlarını veya cihazlarını kayıp, hırsızlık veya hasardan korumak için adımlar atmaları tavsiye edilir.

* Okçu Musa ilkokulu topluluğunun tüm üyelerine, kaybolmaları veya çalınması durumunda telefonlarında veya cihazlarında yetkisiz çağrılar veya eylemlerin gerçekleştirilemediğinden emin olmak için şifre / pin numaralarını kullanmaları önerilir. Şifreler ve pin

numaraları gizli tutulmalıdır. Cep telefonları ve kişisel cihazlar paylaşılmamalıdır.

- Okçu Musa İlkokulu topluluğunun tüm üyelerinin, cep telefonlarının ve kişisel cihazlarının rahatsız edici, aşağılayıcı ya da okul / ayar politikalarına ters düştüğü düşünülen herhangi bir içerik içermediğinden emin olmaları tavsiye edilir.

- Okul / cep telefonları ve cihazları her zaman Kabul Edilebilir Kullanım Politikası ve diğer ilgili politikalara uygun olarak kullanılmalıdır.

- Okul / ebeveynler ve öğrencilerle iletişim kurmak için kullanılan cep telefonları ve cihazları, bir şifre / şifre / pin yoluyla uygun şekilde korunmalıdır ve sadece personel üyeleri tarafından erişilip kullanılmalıdır.

4.3 Kişisel cihazların ve cep telefonlarının kullanımı

4.3 Olası İfadeler:

- Öğrenciler, kişisel cihazların ve cep telefonlarının güvenli ve uygun kullanımı konusunda eğitilecektir.
- Çocukların tüm cep telefonları ve kişisel cihazları, kabul edilebilir kullanım politikasına uygun olarak gerçekleştirilecektir.
- Öğrencinin kişisel cep telefonları ve kişisel cihazları güvenli bir yerde saklanmalı, ders sırasında ve dersler arasında hareket ederken gözden uzak tutulacak ve tutulmayacaktır. (Okula / kuruma uygun şekilde değişiklik yapın)
- Cep telefonları veya kişisel cihazlar, bir personelden izin alınarak onaylanmış ve yönlendirilmiş müfredata dayalı bir faaliyetin bir parçası olmadığı sürece, dersler veya örgün okul saatleri boyunca öğrenciler tarafından kullanılmayacaktır.
- Personelin üyeleri, çocukların cep telefonlarını veya kişisel cihazlarını bir eğitim faaliyeti kapsamında kullanmasına izin vermek için bir eğitim nedenine sahipse, o zaman sadece Liderlik Ekibi tarafından onaylandığında gerçekleşecektir.
- Bir öğrencinin ebeveynleri / bakıcılarıyla iletişim kurması gerekiyorsa, okul / ayar telefonu kullanmalarına izin verilir.
- Ebeveynlere, okul günlerinde çocuklarıyla cep telefonu aracılığıyla değil, okul idaresi ile iletişime geçmeleri tavsiye edilir. İstisnai durumlarda, duruma göre ve anaokulun onayladığı durumlarda istisnalara izin verilebilir.

- Öğrenciler telefon numaralarını sadece güvenilir arkadaşlara ve aile üyelerine vererek koruyabilmelidirler.
- Öğrencilere cep telefonlarının ve kişisel cihazlarının güvenli ve uygun kullanımı konusunda bilgi verilecek ve sınırların ve sonuçların farkına varılacaktır.
- Cep telefonları ve kişisel cihazlar muayene edilmemelidir. Sınav sırasında cep telefonu veya kişisel bir cihaza sahip olan öğrenciler, uygun inceleme kuruluşuna bildirilecektir. Bu, öğrencinin sınavdan ya da tüm sınavlardan çekilmesine neden olabilir.
- Bir öğrenci okul politikasını ihlal ederse, telefon veya cihaza el konulacak ve okul ofisinde güvenli bir yerde tutulacaktır. Cep telefonu ve cihazları, okul politikasına uygun olarak ebeveynlere / bakıcılara bırakılacaktır.
- Okul personeli, bir öğrencinin cep telefonuna ya da cihazına, okul davranışlarına ya da zorbalık politikasına aykırı davranmak için kullanıldığını inanıyorsa ya da cinsel içerikli

gençlik görüntülerini (cinsiyet düşürme) içerebileceğine inandığında el koyabilir. Telefon veya cihaz, Liderlik ekibinin bir üyesi tarafından öğrenci veya ebeveyn / bakıcının rızasıyla aranabilir ve uygunsa silinebilir veya silinmesi istenebilir. Cep telefonu veya kişisel cihaz aramaları sadece okul politikasına uygun olarak gerçekleştirilecektir.

- Bir öğrencinin kişisel cihazındaki veya cep telefonundaki materyallerin yasa dışı olabileceği veya bir suçla ilgili kanıt sağlayabileceğinden şüphe duyulması halinde, cihaz daha fazla araştırma için polise teslim edilecektir.

4.5 Kişisel cihazların ve cep telefonlarının kullanımı

4.5 Olası İfadeler:

- * Personelin, personelin, gençlerin ve ailelerinin profesyonel bir kapasiteye sahip ortam içinde veya dışında iletişim kurmaları için kendi kişisel telefonlarını veya cihazlarını kullanmalarına izin verilmez. Bunu tehlikeye atacak herhangi bir önceden var olan ilişkiler liderler / yöneticilerle tartışılacaktır.

- * Personel, çocukların fotoğraflarını veya videolarını çekmek için cep telefonları, tabletler veya kameralar gibi kişisel cihazları kullanmaz ve sadece bu amaç için iş ekipmanı kullanır.

- * Personel, çocuklarla doğrudan herhangi bir kişisel cihazı kullanmayacak ve sadece dersler / eğitim faaliyetleri sırasında iş ekipmanı kullanacaktır.

- * Personel üyeleri, kişisel telefonların ve cihazların kullanımının her zaman yasaya uygun olarak, örn. ilgili okul politikası ve prosedürlerinin yanı sıra veri koruması, gizlilik, veri güvenliği, Kabul Edilebilir Kullanım vb.

- Personel kişisel cep telefonları ve cihazları ders saatlerinde “sessiz” modda kapalı

/ kapalı konuma getirilecektir.

- Bluetooth veya diğer iletişim biçimleri ders sırasında “gizlenmiş” veya kapalı olmalıdır.
- Acil durumlarda Liderlik Ekibi üyesi tarafından izin alınmadığı sürece, kişisel cep telefonları veya cihazları öğretim periyotlarında kullanılmayacaktır.
- Personel, cep telefonları ve kişisel cihazlar aracılığıyla sitede satın alınan tüm içeriklerin profesyonel rolleri ve beklentileri ile uyumlu olmasını sağlayacaktır.
- Eğer bir personel okul / ayar politikasını ihlal ederse disiplin cezası alınır.
- Bir personelin bir cep telefonunda veya kişisel cihazda saklanan veya saklanan yasadışı içeriğe sahip olduğu veya bir suç işlemiş olduğu düşünüldüğünde, polisle irtibata geçilecektir.
- Cep telefonu veya cihazların kişisel kullanımını içeren personel üyelerine yönelik iddialar, okul / ayar iddiaları yönetim politikasına uygun olarak yanıtlanacaktır.

4.6 Kişisel cihazların ve cep telefonlarının ziyaretçileri

4.6 Olası İfadeler:

- * Ebeveynler / bakıcılar ve ziyaretçiler, cep telefonları ve kişisel cihazları okul / ayarlar kabul edilebilir kullanım politikasına uygun olarak kullanılmalıdır.
- * Ziyaretçilerin ve ebeveynlerin / bakıcıların fotoğraf veya video çekmeleri için cep telefonu veya kişisel cihazların kullanımı okul imajı kullanım politikasına uygun olarak gerçekleştirilmelidir.
- Okul, ziyaretçilere kullanım beklentilerini bildirmek için uygun işaret ve bilgilerin görüntülenmesini sağlayacaktır.
- Personelin, güvenli ve uygun olduğunda endişelere meydan okuması beklenir ve her zaman ziyaretçilerin herhangi bir şekilde kullanımının ihlal edildiğine dair Atanmış Koruma Sorumlusunu bilgilendirir.

5.Politika Kararları

5.1. Çevrimiçi risklerin azaltılması Tüm ayarlar için uygun

5.1 Olası ifadeler:

- * Okçu Musa İlkokulu internetin yeni uygulamalar, araçlar, cihazlar, siteler ve hızlı bir hızla ortaya çıkan malzeme ile sürekli değişen bir ortam olduğunun bilincindedir.
- * Gelişen teknolojiler eğitimsel fayda için incelenecek ve okul liderliği ekibi okulda kullanılmadan önce uygun risk değerlendirmelerinin yapılmasını sağlayacaktır.
- * Okul, personel ve öğrencilerin uygunsuz veya yasa dışı içeriğe erişmesini önlemek için uygun filtreleme ve izleme sistemlerinin uygulanmasını sağlayacaktır. (Okullar, sistemler hakkında uygun

detayları içermelidir)

* Kullanıcıların yalnızca uygun materyallere erişebilmelerini sağlamak için okul tüm makul önlemleri alacaktır. Bununla birlikte, İnternet içeriğinin küresel ve bağlantılı yapısı nedeniyle, uygun olmayan materyallere erişimin bir okul / bilgisayar veya cihaz aracılığıyla asla gerçekleşmeyeceğini garanti etmek her zaman mümkün değildir.

* Okul, çevrimiçi güvenlik (e-Güvenlik) politikasının yeterli olup olmadığını ve politikanın uygulanmasının uygun olup olmadığını belirlemek için teknoloji kullanımını denetleyecektir.

• Çevrimiçi riskleri belirleme, değerlendirme ve en aza indirme yöntemleri, okul liderleri ekibi tarafından düzenli olarak gözden geçirilecektir.

5.2. Daha geniş okul / topluluk ortamında İnternet kullanımı Kendi yerel bağlamındaki tüm ayarlar için uygun

5.2 Olası ifadeler:

• Okul çevrimiçi güvenliğe ortak bir yaklaşım oluşturmak için yerel örgütlerle irtibat kuracaktır.

- Okul, internet kullanımının uygun olduğundan emin olmak için yerel toplulukların ihtiyaçları ile (kültürel geçmişleri, dilleri, dinleri ve etnik kökenleri tanımak dahil) çalışacaktır.
- Okul, okul bilgisayar sistemine veya internete girmesi gereken herhangi bir misafir / ziyaretçi için Kabul Edilebilir Kullanım Politikası sağlayacaktır.

5.3 İnternet erişimini yetkilendirme

İnternet erişimini kolaylaştıran tüm ayarlar için uygun

5.3 Olası ifadeler:

- * Okul, okulun cihazlarına ve sistemlerine erişim izni verilen tüm personel ve öğrencilerin mevcut kaydını tutar.
- * Tüm personel, öğrenciler ve ziyaretçiler herhangi bir okul kaynağını kullanmadan önce Kabul Edilebilir Kullanım Politikasını okuyacak ve imzalayacaktır.
- * Ebeveynlere, yaşlarına ve yeteneklerine uygun gözetimli internet erişimi sağlanacağı konusunda bilgilendirilecek.
- * Ebeveynlerden, öğrenci erişimi için Kabul Edilebilir Kullanım Politikasını okumaları ve gerektiğinde çocuklarıyla tartışmaları istenecektir.
- * Toplumun savunmasız üyelerine (özel eğitim ihtiyaçları olan çocuklarda olduğu gibi) erişim göz önünde bulundurulduğunda, okul, öğrenci (ler) in özel ihtiyaçlarına ve anlayışına dayanarak kararlar alacaktır.

6.Katılım Yaklaşımları

6.1 Çocukların ve gençlerin katılımı

ve eğitimi Tüm ayarlar için uygun

6.1 Olası ifadeler:

- * Öğrenciler arasında güvenli ve sorumlu internet kullanımının önemi hakkında farkındalık yaratmak için, tüm okul boyunca bir online güvenlik (e-Güvenlik) müfredatı kurulacak ve yerleştirilecektir.*
- * Güvenli ve sorumlu kullanımla ilgili eğitim, internet erişiminden önce gelecektir.*
- * Müfredat geliştirme ve uygulama da dahil olmak üzere okul çevrimiçi güvenlik politikaları ve uygulamaları yazılırken ve geliştirilirken öğrencilerden girişler aranır.*
- * Öğrenciler Kabul Edilebilir Kullanım Politikasını yaş ve yeteneklerine uygun bir şekilde okuma ve anlama konusunda desteklenecektir.*
- * Tüm kullanıcılara ağ ve internet kullanımının izleneceği bildirilecektir.*

*Çevrimiçi güvenlik (e-Güvenlik), hem güvenli okul hem de ev kullanımını kapsayan PSHE, SRE, Vatandaşlık ve Bilgi İşlem / ICT programlarına dahil edilecektir.

- İnternet erişimi olan tüm odalarda kabul edilebilir kullanım beklentileri ve posterler yayınlanacaktır.
- İnternet ve teknolojinin güvenli ve sorumlu kullanımı, müfredatta ve tüm konu alanlarında güçlendirilecektir.
- Okul içi çevrimiçi güvenlik (e-Güvenlik) eğitim yaklaşımlarını tamamlamak ve desteklemek için harici destek kullanılacaktır.
- Okul, öğrenciler tarafından teknolojinin pozitif kullanımını ödüllendirecektir.
- Okul, öğrencilerin ihtiyaçlarına uygun olarak çevrimiçi güvenliği geliştirmek için akran eğitimini uygulayacaktır.

6.2 Çocukların ve gençlerin savunmasız olduğu düşünülen

katılım ve eğitim Tüm ayarlar için uygun

6.2 Olası ifade:

* Okçu Musa ilkokulu bazı çocukların bir dizi faktör nedeniyle çevrimiçi olarak daha hassas olduğu düşünülebilir.

6.3 Çalışanların eğitimi ve

eğitimi Tüm ayarlar için

uygun

6.3 Olası ifadeler:

** Çevrimiçi güvenlik (e-Güvenlik) politikası, tüm personel üyeleriyle birlikte resmi olarak sağlanacak ve tartışılacak ve korunma sorumluluklarımızın bir parçası olarak güçlendirilecek ve vurgulanacaktır.*

** Personelimiz internet trafiğimizin izlenebilir ve izlenebilir. Okul sistemlerini ve cihazlarını kullanırken takdir ve profesyonel davranış esastır.*

** Personelin tüm üyeleri için düzenli ve en az yıllık olarak, çeşitli şekillerde, profesyonel ve kişisel olarak güvenli ve sorumlu internet kullanımı için güncel ve uygun personel eğitimi sağlanacaktır.*

** Tüm personel üyeleri, okul dışındaki çevrimiçi davranışlarının okul içindeki rolleri ve itibarlarını etkileyebileceğini fark edeceklerdir. Mesleği ya da kurumu tasfiye*

edebilecekleri ya da profesyonel yeteneklerine olan güveni sarsan bir şey hissedilirse, sivil, hukuki ya da disiplin cezası alınabilir.

- Filtreleme sistemlerini yönetme veya BİT kullanımını izleme sorumluluğu olan personel üyeleri, Liderlik Ekibi tarafından denetlenecek ve sorunları veya endişeleri bildirmek için açık prosedürlere sahip olacaktır.

- Okul / ortam, personelin yaşına ve yeteneklerine göre kullanması gereken faydalı çevrimiçi araçları vurgulayacaktır.

6.4 Ebeveynlerin ve bakıcıların katılımı ve eğitimi Tüm ayarlar için uygun

6.4 Olası ifadeler:

- * Okçu Musa İlkokulu, ebeveynlerin / bakıcıların, çocukların internet ve dijital teknolojinin güvenilir ve sorumlu kullanıcıları olmasını sağlamada önemli bir rol oynadığını kabul eder.

- * Ebeveynlerin dikkati okul çevrimiçi güvenlik (e-Güvenlik) politikası ve bültenler, mektuplar, okul izahnamesi ve okul web sitesinde beklentilerle karşılanacaktır.

- * Evde ve okulda çevrimiçi güvenliğe ebeveynlerle birlikte bir ortaklık yaklaşımı teşvik edilecektir. Bu, ebeveyn evlerinin güvenli ev internet kullanımı için gösteriler ve öneriler sunmayı veya iyi katılımlı diğer etkinliklerde çevrimiçi güvenliği vurgulamayı içerebilir. Ebeveyn akşamları, geçiş olayları, fetuslar ve spor günleri.

- Ebeveynlerin, Ev Okulları Sözleşmesi'nin bir parçası olarak çevrimiçi güvenlik bilgilerini okuması istenecektir.

- Ebeveynler, öğrenciler için Kabul Edilebilir Kullanım Politikasını okuyup çocuklarıyla olan etkilerini

tartışmaya teşvik edilecektir.

- Çevrimiçi güvenliğe sahip ebeveynler için bilgi ve rehberlik, çeşitli biçimlerde ebeveynlere sunulacaktır.
- Ebeveynler, çocukları için çevrimiçi olarak olumlu bir rol modelini teşvik edeceklerdir.

7.Çevrimiçi Kartlara Yanıt Verme ve

Endişelerin Korunması Tüm ayarlar için uygun

Olası ifadeler:

* Topluluğun tüm üyeleri, çevrimiçi / siber zorbalık vb. Dahil olmak üzere karşılaşılabilecek olası çevrimiçi risklerden haberdar olacaktır. Bu, personel eğitimi ve öğrenciler için eğitim yaklaşımları içinde vurgulanacaktır.

- * Okul / topluluk ortamının tüm üyeleri, çevrimiçi güvenlik (e-Güvenlik) endişelerini filtreleme, cinsiyet düşürme, siber zorbalık, yasadışı içerik vb. ihlal etme prosedürleri hakkında bilgilendirilecektir.
- * Belirtilen Korumaya Yönelik Kurşun (DSL), çocuk koruma endişelerini içeren çevrimiçi güvenlik (e-Güvenlik) olaylarından haberdar edilecek ve bunlar kaydedilecektir.
- * İnternet kötüye kullanımı ile ilgili şikayetler, Okul'un şikayet prosedürü kapsamında ele alınacaktır.
- * Çevrimiçi / siber zorbalıkla ilgili şikayetler, okulun taarruz karşıtı politika ve prosedürü kapsamında ele alınacaktır.
- * Personelin kötüye kullanılması ile ilgili şikayete baş öğretmene sevk edilecektir.
- * Öğrenciler, ebeveynler ve personele okulların şikayet prosedürü hakkında bilgi verilecektir.
- * Personel şikayet ve ihbar prosedürü hakkında bilgilendirilecektir.
- * Okul topluluğunun tüm üyeleri, gizliliğin öneminin ve kaygıların bildirilmesi için resmi okul prosedürlerinin izlenmesinin gerekliliğinin farkında olmalıdır.
- * Okul topluluğunun tüm üyeleri çevrimiçi olarak güvenli ve uygun davranışı ve okul topluluğunun diğer üyelerine zarar, sıkıntı veya saldırıya neden olan herhangi bir içerik, yorum, görsel veya video yayınlamamanın önemini hatırlatır.
- * Okul, uygun durumlarda okul disiplini / davranış politikasına uygun olarak çevrimiçi güvenlik (e-Güvenlik) olaylarını yönetecektir.

- * Okul, endişeleri olan herhangi bir olay hakkında ebeveynleri / bakıcıları bilgilendirir.
- * Herhangi bir soruşturma tamamlandıktan sonra, okul öğrenir, öğrenilen dersleri belirler ve gerekli değişiklikleri uygular.
- * Ebeveynler ve çocukların sorunları çözmek için okulla işbirliği içinde çalışması gerekecektir.