TOROSLAR / MERSİN ALİ KUŞÇU ORTAOKULU E-GÜVENLİK POLİTİKASI

1. Çevrimiçi Güvenlik Etik Kuralları Oluşturma

1. *Amaçlar ve politika kapsamı*

1. *Olası beyanlar:*

- ALİ KUŞÇU ORTAOKULU çevrimiçi güvenliğin (e-Güvenlik), bilgisayarlar, tabletler, cep telefonları veya oyun konsolları gibi teknoloji ürünlerini kullanırken, dijital dünyadaki çocukların ve yetişkinlerin korunması için vazgeçilmez bir unsur olduğuna inanmaktadır.
- ALİ KUŞÇU ORTAOKULU internetin ve bilgi iletişim teknolojilerinin günlük yaşamın önemli bir parçası olduğunu belirtir. Dolayısıyla, riskleri yönetmek ve bunlara çözüm üretmek, strateji geliştirmeyi öğrenebilmek ve çevrimiçi ortamda esneklik kazanmak için çocuklar desteklenmelidir.
- ALİ KUŞÇU ORTAOKULU, eğitim standartlarını yükseltmek, başarıyı teşvik etmek, personelin mesleki çalışmalarını desteklemek ve yönetim işlevlerini geliştirmek için topluma kaliteli İnternet erişimi sunma yükümlülüğüne sahiptir.
- ALİ KUŞÇU ORTAOKULU bütün çocukların ve personelin çevrimiçi ortamda potansiyel zararlardan korunmasını sağlamak için belirli bir görevi bulunduğunu belirtir.
- ALİ KUŞÇU ORTAOKULU çevrimiçi güvenlik politikasının amacı şunlardır
    - Toplumun tüm üyelerini ALİ KUŞÇU ORTAOKULU güvenli bir ortam olduğunu temin etmek için, beklenilen anahtar prensipleri, güvenli ve sorumlu kullanım teknolojisi ile ilgili olarak tanımlamak.
    - ALİ KUŞÇU ORTAOKULU topluluğunun tüm üyelerini çevrimiçi olarak korumak ve bu konuda tedbir almak.
    - Bilimin potansiyel riskleri ve bunların yanında yararları konusunda ALİ KUŞÇU ORTAOKULU topluluğunun tüm üyelerinde farkındalık uyandırmak.
    - Tüm personelin güvenli ve sorumlu bir şekilde çalışmasını sağlamak, olumlu online davranışları örnek göstermek ve teknolojiyi kullanırken kendi standartlarını ve uygulamalarını yönetme gerekliliğinin farkında olmak.
    - Topluluğun tüm üyeleri tarafından bilinen çevrimiçi güvenlik endişelerine yanıt verirken kullanılacak prosedürleri açıkça tanımlamak.
- Bu politika, yönetim organlarını, öğretmenleri, destek personelini, vakıfları, ziyaretçileri, gönüllüleri ve okul adına hizmet veren veya bunları yerine getiren diğer kişiler (toplu olarak bu politikada 'personel' olarak anılacaktır) dahil olmak üzere tüm personelin yanı sıra çocuklar, ebeveynleri / bakıcıları kapsamaktadır.
- Bu politika, personel ya da çocuklara sağlanan çalıştıkları dizüstü bilgisayarlar, tabletler veya mobil cihazlar gibi uzaktan kullanım için okul tarafından verilen kişisel cihazlar da dahil olmak üzere bilgi iletişim cihazlarına erişimi ve internet erişimini sağlar.
- Bu politika, koruma ve çocuk koruma, zorbalığa maruz kalma, davranış, veri güvenliği, görüntü kullanımı, Kabul Edilebilir Kullanım Politikaları, gizlilik, tarama, arama ve müsadere ve ilgili müfredat dahil olmak üzere diğer ilgili okul politikaları ile birlikte okunmalıdır. Bilişim / BİT, Kişisel Sosyal ve Sağlık Eğitimi, Vatandaşlık ve Cinsellik ve İlişkiler Eğitimi gibi politikalar.

1.2 Çevrimiçi güvenlik politikası yazma ve gözden geçirme

1. *Olası beyanlar:*

E-Safety Güvelik Ekibi : Ahmet Arıkan, Fatma Nazik Esenboğa, Sevda Yeniçıkan Faydaver

Okulun güvenliği (eGüvenliği)

Okul müdürü tarafından onaylanan politika:.

Tarih: 11/09/2019

- ALİ KUŞÇU ORTAOKULU Online (çevrimiçi) güvenlik politikası, personel, öğrenciler ve ebeveynleri / bakıcıları içeren, gerektiğinde uzman tavsiyesi ve katkısı ile Müdür Yardımcısı Ahmet Arıkan (Başkan) Bilişim Öğretmeni Fatma Nazik Esenboğa (Üye), ve İngilizce Öğretmeni Sevda Faydaver (Üye) den oluşan e-güvenlik yönetim ekibi tarafından yazılmıştır. (E-Güvenlik Yönetim ekibi 2019-2020 Eğitim-Öğretim yılı 1.dönem 1.Öğretmenler Kurul toplantısında alınan kararla oluşturulmuştur.)

- Okul e çevrimiçi güvenlik sorumlusu olarak Fatma Nazik Esenboğa'yı ve Sevda Yeniçıkan Faydaver*'i* atadı .
- Okul, online güvenlik (e-Güvenlik) baş sorumluluğuna e-güvenlik yönetim ekibi başkanı olarak Müdür Yardımcı Ahmet Arıkan'ı atandı.
- Çevrimiçi güvenlik (e-Güvenlik) Politikası ve uygulaması, en az yılda bir kez veya gerekirse daha erken bir tarihte okul idaresi ve kurul tarafından gözden geçirilecektir.

1.3 Topluluk için kilit sorumluluklar

1. *Okul / belirleme yönetimi ve liderlik ekibinin başlıca sorumlulukları şunlardır:*

- Çevrimiçi güvenlik vizyonunu ve kültürünü, okul topluluğu genelinde uygun destek ve istişarede bulunarak ulusal ve yerel tavsiyeler doğrultusunda tüm paydaşlara geliştirmek, sahip olmak ve bunları teşvik etmek.

- Çevrimiçi güvenliğin güçlü bir çevrimiçi güvenlik kültürü proaktif olarak incelenmesini tüm toplum tarafından bir korunma meselesi olarak görülmesini sağlamak.
- Tüm toplumun çevrimiçi güvenlik rolü ve sorumluluklarını yerine getirmek için yeterli zaman ve kaynağa sahip olmalarını sağlayarak Belirlenmiş Koruyucu Tedbirler Öncülüğünü (DSL) desteklemek.

- Çevrimiçi güvenlikle ilgili uygun profesyonel davranışı ve teknolojinin kullanımını kapsayan Kabul Edilebilir Kullanım Politikası da dahil olmak üzere uygun ve güncel politikaların ve prosedürlerin bulunmasını sağlamak.

- Çocukların gerekli eğitim materyallerine erişmesini sağlamak için okul toplumunun ihtiyaçlarını karşılayan uygun olmayan içerikten çocukları korumak için uygun ve uygun filtreleme ve izleme sistemlerinin kurulmasını sağlamak.
- Okul sistemlerinin ve ağlarının güvenliğini izlemek ve okul / ayar ağ sisteminin etkin bir şekilde izlenmesini sağlamak için teknik personel ile birlikte çalışmak ve destek sağlamak.
- Tüm personel üyelerinin, çevrimiçi güvenlik rolleri ve sorumlulukları ile ilgili düzenli, güncel ve uygun eğitim almalarının sağlanması ve uygun güvenli iletişimle ilgili rehberlik sağlanması.
- Çevrimiçi güvenliğin tüm öğrencilere çevrimiçi güvenliği, ilgili riskleri ve güvenli davranışları yaşa uygun bir şekilde anlamasını sağlayan yenilikçi bir okul / öğretim müfredatı içerisinde yer almasını sağlama.
- Çevrimiçi güvenlik olaylarından haberdar olmak ve diğer kurumların ve desteğin uygun şekilde irtibatlandırılmasını sağlamak.
- Çevrimiçi korunma kayıtlarını almak ve düzenli olarak gözden geçirmek ve bunları gelecekte kullanmak üzere şekillendirmek için kullanmak.
- Okul, yerel ve ulusal destek dahil olmak üzere çevrimiçi güvenlik endişeleri ile ilgili olarak okul / çevre topluluğunun erişebilmesi için sağlam raporlama kanallarının bulunmasını sağlamak.
- Cihazların güvenli ve sorumlu kullanılmasını sağlamak da dahil olmak üzere, teknolojinin güvenli kullanımı ile ilgili uygun risk değerlendirmelerinin yapılmasını sağlamak.
- Yönetim Organı üyesinin çevrimiçi güvenliğin sağlanmasına ilişkin sorumlu olduğunu belirtmek.

- İyileştirme alanlarını güçlendirmek ve belirlemek için mevcut çevrimiçi güvenlik uygulamasını denetlemek ve değerlendirmek.
- E-Güvenlik yönetim ekibinin çevrimiçi güvenlik sorumlusu ile birlikte çalışmasını sağlamak. (Aynı kişi değillerse, bkz. Bölüm 1.3.2)

1.3.2 Belirlenmiş Koruyucu Kurşunun temel sorumlulukları şunlardır:

- Tüm çevrimiçi korunma konularında adlandırılmış bir irtibat noktası olarak hareket etmek ve diğer personel üyeleri ve diğer ajanslarla uygun şekilde iletişime geçmek.
- Çevrimiçi güvenlikle ilgili mevcut araştırma, mevzuat ve eğilimlerle günce tutmak.
- Olumlu çevrimiçi davranışı teşvik etmek için yerel ve ulusal etkinliklere katılımı koordine etmek, örneğin Güvenli İnternet Günü.
- Çevrimiçi güvenliğin çeşitli kanallar ve yaklaşımlar vasıtasıyla ebeveynlere, bakıcılara ve daha geniş topluluğa terfi edilmesini sağlama.
- Uygulamanın mevcut mevzuata uygun olmasını sağlamak için veri koruma ve veri güvenliği için okul idaresiyle birlikte çalışmak.
- Çevrimiçi güvenlik endişelerinin / olaylarının ve kayıt yapılarını ve mekanizmalarını koruyan okulların bir parçası olarak alınan önlemlerin kayıtlarının tutulması.
- Gözardı edilen noktaları belirlemek için Çevrim içi güvenlik olaylarını izlemek, belirtmek ve bu bilgileri okuldaki eğitim ihtiyacına bağlı olarak güncellemek.
- Okul idaresine, Yönetim Organına ve diğer acentelere, çevrimiçi güvenlik endişeleri ve yerel veriler / rakamlar hakkında rapor vermek .
- Yerel ve ulusal kurumlarla irtibat kurmak.

- Paydaşların katılımı ile düzenli olarak çevrimiçi güvenlik politikalarını, Kabul Edilebilir Kullanım Politikalarını (AUP'ler) ve diğer ilgili politikaları gözden geçirmek ve güncellemek için okul yönetimiyle birlikte çalışmak (en az yılda bir kez).
- Çevrimiçi güvenliğin diğer uygun okul politikaları ve prosedürleriyle bütünleştirilmesini sağlama.

1.3.3 Tüm çalışanların kilit sorumlulukları şunlardır:

- Çevrimiçi güvenlik politikalarının geliştirilmesine katkıda bulunmak.
- Okul Kabul Edilebilir Kullanım Politikalarını okumak (AUP'lar) ve onlara bağlı kalmak.
- Okul / tesisat sistemlerinin ve verilerin güvenliğinden sorumlu almak.
- Bir dizi farklı çevrimiçi güvenlik konusundaki farkındalığa sahip olmak ve onların bakımında çocuklarla nasıl ilişkili olabileceklerini bilmek.
- Yeni ve gelişmekte olan teknolojiler kullanıldığında iyi uygulamaları modellemek.
- Mümkün olan yerlerde müfredat teslimatı için çevrimiçi güvenlik eğitimi almak.
- 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 gündeme getirmeyi bilmek.
- Çevrimiçi güvenlik konularda, dahili ve harici olarak, uygun desteğin verilebileceğini temin etmek.
- Kişisel teknoloji kullanımlarında, harici ve dahili alanda profesyonel bir davranış tutumunun korunması.

- Olumlu öğrenme fırsatlarına vurgu yapılması.
- Bu alanda mesleki gelişim için kişisel sorumluluk alınması.

1.3.4 Yukarıdakilere ilaveten, teknik ortamı yöneten personelin başlıca sorumlulukları şunlardır:

- Öğrenme fırsatlarının en üst düzeye çıkartılmasını sağlarken güvenli online uygulamalarını destekleyen güvenli bir teknik altyapının sağlanması.
- Yönetim ekibi ile ortaklaşa sistemlerin ve verilerin emniyetli bir şekilde uygulanmasının sorumluluğunu üstlenmek.
- Okullara ait cihazlarda tutulan kişisel ve hassas bilgileri korumak için uygun erişim kontrollerinin ve şifrelemenin uygulanmasını sağlamak.
- Okul filtreleme politikasının düzenli olarak uygulanması ve güncellenmesinin sağlanması ve uygulanmasına ilişkin sorumluluğun DSL ile paylaşılması.
- Okul ortak ağının düzenli olarak izlenmesini sağlamak ve kasıtlı ya da yanlışlıkla yapılan kullanımları DSL'ye bildirmek.
    - Herhangi bir ihlal veya endişeyi e-güvenlik yönetim ekibine ve idareye rapor etmek ve bu raporların birlikte kaydedilmesini ve uygun önlemlerin tavsiye edildiği şekilde alınmasını sağlamak.
- Teknik altyapının güvenliği ile ilgili olarak ilgili mevzuat hakkında anlayış geliştirmek.
- Herhangi bir ihlali bildirmek ve yerel otorite (veya diğer yerel veya ulusal kurumlar) ile teknik altyapı konularında irtibat kurun.

- Özellikle uygun çevrimiçi güvenlik politikaları ve prosedürlerinin geliştirilmesi ve uygulanmasında e-güvenlik yönetim ekibine teknik destek ve perspektif sağlamak.

- Okulun BİT altyapısının / sisteminin güvenli olduğunu ve kötüye kullanım veya kötü niyetli saldırılara açık olmamasını sağlamak.
- Tüm ayarlama makinelerinde ve taşınabilir aygıtlarda uygun anti-virüs yazılımının ve sistem güncellemelerinin kurulup kurulmadığından emin olmak.
- Güçlü parolaların en genç kullanıcılar hariç tüm kullanıcılara uygulandığından ve emin olmak

1.3.5 Çocukların ve gençlerin başlıca sorumlulukları şunlardır:

- Çevrimiçi güvenlik politikalarının geliştirilmesine katkıda bulunmak.
- Okul Kabul Edilebilir Kullanım Politikalarını okumak (AUP'lar) koymak 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.

Kişisel 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 alakalı kendi farkındalık ve öğrenimlerinden sorumlu olmak.
- Belli bir teknolojiyi kullanmanın kişisel risklerini değerlendirmek ve bu riskleri sınırlamak için güvenilir ve sorumluluk sahibi olmak.

1.3.6 Ebeveynlerin ve bakıcıların başlıca sorumlulukları şunlardır:

- Okul Kabul Edilebilir Kullanım Politikalarını okumak, belirlemek, çocuklarını kendilerine bağlı kalmaya teşvik etmek ve uygun olduğunda kendilerini de bu politikalara adamak.
- Çocuklarıyla çevrimiçi güvenlik konularını tartışmak, okulun çevrimiçi güvenlik yaklaşımlarını desteklemek ve evde uygun güvenli çevrimiçi davranışları pekiştirmek.
- Teknoloji ve sosyal medyanın güvenli ve uygun kullanımına rol model olmak.
- Davranışlarında, çocuğunun çevrimiçi olarak zarar görme tehlikesi altında olduğunu gösteren değişiklikleri belirlemek.
- Okul veya diğer uygun kurumlardan, çevrimiçi problem veya endişelerle 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.

2. Çevrimiçi İletişim ve Teknolojinin Daha Güvenli Kullanımı

2.1 Okul / web sitesinin yönetilmesi

Olası beyanlar:

- Web sitesindeki 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 için hasar görmemek için (örn. '@' Yerine 'AT' yazısı girilerek) e-posta adresleri çevrimiçi olarak dikkatli bir şekilde yayınlanacaktır.
- Öğrenci çalışmaları izniyle ya da ebeveynlerinin / bakıcılarının izniyle yayınlanacaktır.
- Okul web sitesinin yönetici hesabı, uygun bir şekilde şifrelenerek korunacaktır.
- Okul, çevrimiçi güvenlik dahil olmak üzere, toplumun üyeleri için okul web sitesinde korunma hakkında bilgi yayınlayacaktır.

2.2 Çevrimiçi görüntü ve videolar yayınlama

Olası beyanlar:

- Okul, çevrimiçi paylaşılan tüm resimlerin ve videoların okul resim kullanımı politikasına uygun şekilde kullanılmasını sağlayacaktır.
- Okul idaresi, 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 ebeveynlerin veya bakıcıların yazılı izni her zaman elde edilecektir.

2.3 E-postaları yönetme

Tüm ayarlar için önemlidir

2.3 Olası beyanlar:

- Öğrenciler eğitim amacıyla yalnızca okul e-posta hesapları kullanabilirler.
- Personelin tüm üyelerine resmi bir iletişim için kullanılacak belirli bir okul e-posta adresi verilir.
- Kişisel e-posta adresinin personel tarafından bir kurum veya kuruluş için kullanılması yasaktır.
- Mesaj ve e-posta zincirleri yasaktır. Spam veya önemsiz posta engellenecek ve e-posta sağlayıcısına bildirilecektir.
- Veri koruma mevzuatına tabi olabilecek herhangi bir içeriği (örn. Hassas veya kişisel bilgiler) içeren herhangi bir elektronik iletişim yalnızca güvenli ve şifrelenmiş bir e-posta ile gönderilecektir.
- Okul e-posta sistemlerine erişim her zaman veri koruma yasalarına uygun olarak ve diğer okul politikalarına (örn. Gizlilik) uygun olarak gerçekleşecektir.

- Topluluk üyeleri, saldırgan bir iletişim kurdukları takdirde derhal belirlenmiş bir personele haber vermekle yükümlüdürler ve bu dosyalar okulun dosyalarında / kayıtlarında korunacaktır.

- Okul dışındaki iletişim için tüm sınıf veya grup e-posta adresleri kullanılabilir.
- Personel, e-postaya yanıt verirken, özellikle personel, öğrenciler ve ebeveynler arasında iletişim kurulması halinde, uygun bir iş hayatı dengesi geliştirmeye teşvik edilecektir.
- Aşırı sosyal e-posta kullanımı öğretme ve öğrenmeyi etkileyebilir ve bu nedenle kısıtlanabilir. Okuldaki harici kişisel e-posta hesaplarına erişim engellenebilir.
- Dış organizasyonlara gönderilen e-postalar gönderilmeden önce izin verilmeli ve dikkatli yazılmalı, okul tarafından yazılan bir mektup da aynı şekilde dikkatlice yazılmalıdır.
- Okul, gelişim meselelerini bildiren özel bir e-postaya sahip olacaktır. Bu gelen kutusu, belirlenmiş ve eğitimli personel tarafından yönetilecektir.
- Okulun e-posta adresleri ve diğer resmi iletişim bilgileri, kişisel sosyal medya hesapları oluşturmak için kullanılamaz.

2.4 Eğitim amaçlı resmi video konferans ve web kamerası kullanımı

2.4 Olası beyanlar:

- Okul, video konferansın çok çeşitli öğrenme avantajlarıyla zorlu bir faaliyet olduğunu kabul eder. Hazırlık ve değerlendirme, tüm faaliyet için gereklidir.
- Video konferans ekipmanlarının hepsi kullanılmadığında ve mümkün olduğu yerde, otomatik cevaplamaya ayarlanmadığında kapatılacaktır.

- Harici IP adresleri diğer sitelere sunulmayacaktır.
- Video konferans iletişim detayları kamuoyuna açıklanmayacaktır.
- Video konferans ekipmanları güvenli bir şekilde tutulacak ve gerekirse kullanılmadığında kilitlenecektir.
- Okul video konferans ekipmanları izinsiz olarak okul binalarından alınmayacaktır.
- Personel, dış video konferans fırsatlarının ve / veya araçlarının uygun bir şekilde değerlendirildiğinden emin olacak ve olaylara erişmek için kullanılan hesapların ve sistemlerin uygun bir şekilde güvenli olmasını sağlayacaktır.

Kullanıcılar

- Öğrenciler, bir video konferans araması veya mesajı hazırlamadan veya cevaplamadan önce bir öğretmenin iznini istemelidir.

- Video konferans, öğrencilerin yaşı ve yeteneği için uygun bir şekilde denetlenecek.
- Veliler ve bakıcıların rızası, çocuklar video konferans faaliyetlerine katılmadan önce alınmalıdır.
- Video konferans, güvenilir bir risk değerlendirmesini takiben, resmi ve onaylanmış iletişim kanalları vasıtasıyla gerçekleşecektir.

- Sadece ana yöneticilere video konferans yönetim alanlarına veya uzaktan kumanda sayfalarına erişim hakkı verilmektedir.

- Eğitici video konferans servisleri için özgün oturum açma ve şifre bilgileri yalnızca personel üyelerine verilecek ve güvence altına alınmış olacak.

içerik

- 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 kurmalıdır. Okul değilse bu katılımcı, sınıf için uygun olan materyali teslim alıp almadığı kontrol edilmelidir.

2.5 İnternetin ve ilgili cihazların uygun ve güvenli derslik kullanımı

2.5 Olası beyanlar:

- İnternet kullanımı eğitime erişimin önemli bir özelliğidir ve tüm çocuklar okul müfredatının bir parçası olarak endişelere cevap vermek için stratejiler geliştirmelerini destekleyecek ve onlara yardımcı olacak yaşa ve yeteneğe uygun eğitim alacaklardır. Daha fazla bilgi için lütfen özel müfredat politikalarına erişin.
- Okulun internet erişimi eğitimi geliştirmek ve genişletmek için tasarlanacaktır.
- İnternet erişim seviyeleri müfredat gerekliliklerini ve öğrencilerin yaş ve yeteneklerini yansıtacak şekilde gözden geçirilecektir.
- Tüm personel, çocukları korumak için sadece filtrelemeye güvenmemelerinin farkındadır ve gözetim, sınıf yönetimi ve güvenli ve sorumlu kullanım eğitimi önemlidir.
- Öğrencilerin gözetimi yaşlarına ve yeteneklerine uygun olacaktır.
  - Genç öğrencilerin İnternet'e erişimi, yetişkinlerin göstermesiyle, öğrencilerin yaşı ve yeteneği için planlanan öğrenme çıktılarını destekleyen belirli ve onaylanmış çevrimiçi materyallere doğrudan denetlenen erişimle sağlanacaktır.
  - 8-11 yaşındaki öğrenci denetlenecek. Öğrenciler yaşa uygun arama motorlarını ve çevrimiçi araçları kullanacak ve çevrimiçi etkinlikler gerektiğinde öğretmen tarafından yönlendirilecek. Çocuklar, öğrencilerin yaşı ve yeteneği için planlanan öğrenme çıktılarını destekleyen çevrimiçi materyal ve kaynaklara yönlendirilecektir.
  - Yetenek ve anlayışlarına göre, genç öğrenciler teknoloji kullanırken eğitime uygun bir şekilde gözetim altına alınacaklardır.
- Okula ait tüm 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 önermeden daima gözden geçirmelidirler.
- Öğrenciler, bilginin konumlanması, alınması ve değerlendirilmesi becerileri de dahil olmak üzere, etkili İnternet kullanımı konusunda eğitilecektir.
- Okul, personelin ve öğrencilerin İnternet kaynaklı materyallerin telif hakkı yasalarına uygun olmasını ve bilgi kaynaklarını kabul etmesini sağlayacaktır.

- Öğrencilere, okudukları ve öğrenecekleri materyallerin direkt doğruluğunu kabul etmeden önce eleştirel bir biçimde doğrulanması gerektiği gösterilecektir.
- Çevrimiçi materyallerin değerlendirilmesi, her konuda öğretme ve öğrenmenin bir parçasıdır ve müfredatta okulun sorumluluğu olarak görülür.
- Okul, öğrencileri ve çalışanlarının güvenli bir ortamda iletişim kurmalarını ve işbirliği yapmalarını sağlamak için interneti kullanacaktır.

3. Kişisel Cihazların ve Cep Telefonlarının Kullanımı

Tartışma:

3.1 Kişisel cihazlar ve cep telefonları ile ilgili gerekçe

3.1 Olası Bildirimler:

- Cep telefonlarının ve diğer kişisel cihazların çocuklar, yetişkinler ve gençler arasında yaygın bir şekilde kullanılması ALİ KUŞÇU ORTAOKULU topluluğunun cep telefonlarının ve kişisel cihazların sorumlu bir şekilde kullanılmasını sağlamak için gerekli adımları atmalarını gerektirir.
- Gençlerin ve yetişkinlerin cep telefonlarının ve diğer kişisel cihazların kullanımı, okul idaresi tarafından kararlaştırılacak ve okul Kabul Edilebilir Kullanım veya Cep Telefonu Politikası dahil olmak üzere gerekli politikalarda yer alacaktır.
    - ALİ KUŞÇU ORTAOKULU, mobil teknolojilerle yapılan kişisel iletişimin, çocuklar, personel ve anne-baba / bakıcılar için gündelik yaşamın kabul edilen bir parçası olduğunun farkındadır; ancak, bu tür teknolojilerin okul ortamında güvenli ve uygun bir şekilde kullanılmasını gerektirir.

3.2 Kişisel cihazların ve cep telefonlarının güvenli bir şekilde kullanılması için beklentiler

3.2 Olası Bildirimler:

- Kişisel cihazların ve cep telefonlarının tümü yasaya ve diğer okul politikalarına *uygun olarak* eğitime dahil edilmelidir.
- Okula getirilen her türlü elektronik cihazın sorumluluğu kullanıcıya aittir. Okul, bu tür öğelerin kaybolması, çalınması veya zarar görmesi konusunda sorumluluk kabul etmez. Okul bu tür cihazların potansiyel veya fiili neden olabileceği 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 yasaklanmış ve herhangi bir ihlal, disiplin / davranış politikasının bir parçası olarak ele alınacaktır.
    - ALİ KUŞÇU ORTAOKULU topluluğunun tüm üyelerine cep telefonlarını veya cihazlarını kayıp, hırsızlık veya hasardan korumak için adım atmaları önerilir.
    - ALİ KUŞÇU ORTAOKULU topluluğunun tüm üyelerinden, cihazlarının kaybolması veya çalınması durumunda 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.

- ALİ KUŞÇU ORTAOKULU topluluğunun tüm üyelerine, cep telefonlarının ve kişisel cihazlarının saldırgan, küçümseyen veya başka şekilde okul politikalarına aykırı düşen herhangi bir içerik içermediğinden emin olmaları önerilir.

3.3 Öğrencilerin kişisel cihazların ve cep telefonlarının kullanımı

3.3 Olası Bildirimler:

- Öğrenciler, kişisel cihazların ve cep telefonlarının güvenli ve uygun kullanımı konusunda eğitim alacaklardır.
- Çocukların cep telefonlarının ve kişisel cihazların tüm kullanımları, kabul edilebilir kullanım politikasına uygun olarak gerçekleşecektir.
- Cep telefonları veya kişisel cihazlar, öğrencilerin bir öğretim üyesinin onayını almadan yönlendirilmiş müfredat tabanlı etkinlik kapsamında olmadıkları sürece, dersler veya resmi okul saatlerinde öğrenciler tarafından kullanılamaz.
- Personel üyelerinin, çocukların cep telefonlarını veya kişisel cihazlarını bir eğitim etkinliği kapsamında kullanmalarına izin vermek için eğitimsel bir nedeni varsa, bu yalnızca Okul müdüriyeti tarafından onaylandığında gerçekleşecektir.
- Bir öğrencinin ebeveynlerine / bakıcılarına başvurması gerekiyorsa, okul telefonunu kullanmasına izin verilecektir.
- Ebeveynlerin ders saatlerinde cep telefonuyla çocuklarıyla iletişim kurmamaları, okul ofisine başvurmaları önerilir. İstisnai durumlarda ve öğretmenin onayıyla kullanıma izin verilebilir.
- Öğrenciler, telefon numaralarını yalnızca güvenilir arkadaşlarına ve aile üyelerine vererek korunmalıdır.
- Öğrencilere, cep telefonlarının ve kişisel cihazların güvenli ve uygun bir şekilde kullanımı öğretilecek ve sınırların ve sonuçlarının farkındalığı aşılanacaktır.
- Okul personeli, okul davranışını veya zorbalık politikasını ihlal etmek için kullanıldığına veya gençlerin ürettiği cinsel imgeler içerebileceğine inanıyorsa, bir öğrencinin cep telefonuna veya cihazına el koyabilir. Telefon veya cihaz, öğrencinin veya veli / bakıcının onayı ile idarenin bir üyesi tarafından aranabilir ve uygunsa, içerik silinebilir veya silinmek üzere talep edilebilir. Cep telefonu veya kişisel cihazların aranması yalnızca okul politikasına uygun olarak yapılacaktır.
- 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.

3.4 Personelin cihaz ve cep telefonlarının kullanımı

3.4 Olası Bildirimler:

- Personelin, kendi kişisel telefonlarını veya cihazlarını, çocukların, gençlerin ve ailelerinin, mesleki bir ortamın içinde veya dışındaki bölgeleriyle bağlantı kurmalarına izin verilmez. Bu konuda anlaşmaya varma için yöneticilerle görüşülmelidir.
- Personel, çocukların fotoğraflarını veya videolarını çekmek için cep telefonları, tabletler veya kameralar gibi kişisel cihazları kullanamaz ve yalnızca bu amaç için sağlanan ekipmanı kullanır.
- Personel herhangi bir kişisel cihazı doğrudan çocuklarla kullanamaz ve ders / eğitim etkinlikleri sırasında yalnızca iş tarafından sağlanan ekipmanı kullanır.
- Personel üyeleri, kişisel telefonların ve cihazların herhangi bir şekilde kullanımının daima veri koruma ve ilgili okul politikası ve prosedürleri (örn. Gizlilik, veri güvenliği, Kabul Edilebilir Kullanım vb .) *Gibi* yasa uyarınca yerine getirilmesini sağlayacaktır.

- Personel kişisel cep telefonları ve cihazları ders saatlerinde kapatıp / sessiz moda geçirir.
- Bluetooth veya diğer iletişim biçimleri ders saatlerinde "gizlenmiş" veya kapalı olmalıdır.
- Acil durumlarda yönetimin bir üyesi tarafından izin verilmemişse, kişisel cep telefonları veya cihazları öğretim dönemleri boyunca kullanılamaz.
- Bir personelin okul / ilke 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.

3.5 Ziyaretçilerin kişisel cihazları ve cep telefonlarını kullanımı

3.5 Olası Bildirimler:

- Ebeveynler / bakıcılar ve ziyaretçiler, okul kabul edilebilir kullanım politikasına uygun olarak cep telefonlarını ve kişisel cihazları kullanmalıdır.
- Fotoğraflar veya videolar çekmek için ziyaretçiler, ebeveynler / bakıcılar tarafından cep telefonlarının veya kişisel cihazların kullanılması, okul resmi kullanımı politikasına uygun olarak gerçekleştirilmelidir.

- Okul, ziyaretçilere kullanım şartlarını bildirmek için uygun tabela ve bilgileri sağlayacak ve sunacaktır.
- Personelin, endişeleri güvende ve uygun olduğunda bildirmesi beklenir ve her zaman ziyaretçilerin herhangi bir ihlalini Belirlenmiş Korunma kanununa bildireceklerdir.

4. Politika Kararları

4.1. Çevrimiçi riskleri azaltmak

4.1 Olası beyanlar:

- ALİ KUŞÇU ORTAOKULU internetin yeni uygulamalar, araçlar, cihazlar, siteler ve materyallerin hızla geliştiği sürekli değişen bir ortam olduğunun farkındadır.

- Gelişen teknolojiler eğitsel fayda açısından incelenecek ve okul idaresi, okulda kullanılmadan önce uygun risk değerlendirmelerinin yapılmasına izin verecektir.
- Okul, personelin ve öğrencilerin uygun olmayan veya yasadışı içeriğe erişmesini önlemek için uygun filtreleme ve izleme sistemlerinin kurulmasını sağlayacaktır.
- Okul, kullanıcıların yalnızca uygun materyallere erişmesini sağlamak için makul önlemleri alacaktır. Bununla birlikte, internet içeriğinin küresel niteliğinden dolayı, uygun olmayan materyallerin bir bilgisayar ya da cihaz vasıtasıyla okulda hiçbir zaman bulunmayacağını garanti etmek her zaman mümkün değildir.
- Okul, çevrimiçi güvenlik (e-Güvenlik) politikasının yeterli olup olmadığını ve politikanın uygulanmasının uygun olup olmadığını belirlemek için teknolojinin kullanımını denetleyecektir.

- Çevrimiçi riskleri belirleme, değerlendirme ve azaltma yöntemleri okul idaresi tarafından düzenli olarak incelenecektir.

4.2. Daha geniş çapta okul / toplum ortamında internet kullanımı

4.2 Olası beyanlar:

- Okul, çevrimiçi güvenlik konusunda ortak bir yaklaşım oluşturmak için yerel kuruluşlarla irtibat kuracak.
- Okul, internet kullanımının uygun olmasını sağlamak için yerel topluluğun ihtiyaçları (kültürel geçmişleri, dilleri, dinleri ve etnik kökenleri tanımayı da içeren) ile uyumlu olacaktır.
- Okul, okul bilgisayar sistemine veya sitedeki internete erişmesi gereken herhangi bir konuk / ziyaretçi için Kabul Edilebilir Kullanım Politikası sağlayacaktır.

4.3 İnternet erişiminin yetkilendirilmesi

4.3 Olası beyanlar:

- Okul, okulun cihaz ve sistemlerine erişim izni verilen tüm personelin ve öğrencilerin güncel bir kaydını tutacaktır.
- Tüm personel, öğrenciler ve ziyaretçiler, herhangi bir okul kaynaklarını kullanmadan önce Kabul Edilebilir Kullanım Politikasını okuyacak ve imzalayacaklardır.
- Ebeveynlere, öğrencilere, yaşlarına ve yeteneklerine uygun denetlenen İnternet erişimi sağlanacağı bildirilecektir.
- Ebeveynlerden, öğrencilerin erişebilmesi için Kabul Edilebilir Kullanım Politikasını okumaları ve uygun olduğunda, çocuklarıyla tartışmaları istenecektir.
- Toplumun savunmasız üyeleri için (özel eğitim gereksinimi olan çocuklar gibi) internet erişimi düşünürken, okul öğrencilerin belirli ihtiyaçları ve anlayışları temelinde kararlar alacaktır.

5. Katılım Yaklaşımları

- 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 girdileri 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, Citizenship and Computing / BİT programlarına dahil edilecek ve hem güvenli okul hem de evde kullanımını kapsayacaktır.

- Kabul Edilebilir Kullanım beklentileri ve Postalar, Internet erişimi olan tüm odalarda yayınlanacaktır.
- İnternetin ve teknolojinin güvenli ve sorumlu kullanımı, müfredatta ve tüm konularda pekiştirilmelidir.
- Dışarıdan destek, okulların dahili çevrimiçi güvenlik (e-Güvenlik) eğitim yaklaşımlarını tamamlamak ve desteklemek için kullanılacaktır.
- Okul, öğrencilerin teknolojiyi olumlu şekilde kullanımlarını ödüllendirecektir.
- Okul, öğrencilerin ihtiyaçlarına uygun olarak çevrimiçi güvenliği geliştirmek için akran eğitimini uygulayacaktır.

5.2 Savunmasız kabul edilen çocukların ve gençlerin katılımı ve eğitimi

5.2 Olası ifade:

- ALİ KUŞÇU ORTAOKULU, bir takım faktörlerden dolayı bazı çocukların çevrimiçi ortamda daha savunmasız olduğunu düşünmektedir.

5.3 Personelin katılımı ve eğitimi

5.3 Olası beyanlar:

- 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 tek bir kullanıcıya kadar izlenebileceğinin farkındadır. Okul sistemlerini ve cihazlarını kullanırken takdir yetkisi ve profesyonel davranış gereklidir.
- Personelin tümüne, profesyonel ve kişisel olarak, güvenli ve sorumlu İnternet kullanımı konusunda güncel ve uygun personel eğitimi, düzenli (en az yıllık) temelde çeşitli şekillerde sağlanacaktır.
- Çalışanların tümü, çevrimiçi davranışlarının okuldaki rolü ve itibarını etkileyebileceğinin farkına varacaktır. Mesleği veya kurumu güç duruma düşürdüğü veya profesyonelliğe aykırı bir halin bulunduğu düşünülürse, hukuk veya disiplin önlemleri alınabilir.

- Filtreleme sistemlerini yönetme veya BİT kullanımını izleme sorumluluğu taşıyan personelin üyeleri, idare 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.

5.4 Anababalar ve bakıcıların katılımı ve eğitimi

5.4 Olası beyanlar:

- ALİ KUŞÇU ORTAOKULU, çocukların internetin ve dijital teknolojinin güvenilir ve sorumlu kullanıcıları olabilmeleri için ana-babanın / bakıcıların oynayacakları önemli bir role sahip olduklarını kabul eder.
- Ebeveynlerin dikkatleri, bültenler, mektuplar, okul izahname ve okul web sitesinde okul çevrimiçi güvenlik (e-Güvenlik) politikasına ve beklentilerine yöneltilmelidir.
- Evde ve okulda ebeveynlerle çevrimiçi güvenlik konusunda ortaklık yaklaşımı teşvik edilecektir. Bu, güvenli ana sayfa İnternet kullanımı için gösteriler ve öneriler içeren ebeveyn akşamları sunumları veya bayramlar ve spor günleri gibi diğer etkinliklerde çevrimiçi güvenliğin vurgulanmasını içerebilir.

- Veli-Okul Anlaşması'nın bir parçası olarak ebeveynlerin çevrimiçi güvenlik bilgilerini okumaları istenecektir.
- Ebeveynler, Okula Kabul Edilebilir Kullanım Politikasını okumaya ve çocuklarıyla etkilerini tartışmaya teşvik edilecektir.
- Çevrimiçi güvenlik konusunda ebeveynler için bilgi ve rehberlik, çeşitli biçimlerde sunulacaktır.
- Ebeveynlerin, çevrimiçi olarak çocukları için rol model olacak olumlu davranışları teşvik edilecektir.

6. Çevrimiçi Olaylara Yanıt Verme ve Endişeleri Koruma

Olası beyanlar:

- Topluluğun tüm üyeleri, cinsel tercih, çevrimiçi / siber zorbalık gibi karşılaşılabilecek çevrimiçi risklerin çeşitliliğinden haberdar edilecektir. Bu, öğrencilere yönelik personel eğitimi ve eğitim yaklaşımları içerisinde vurgulanacaktır.
- Okul topluluğunun tüm üyeleri, filtreleme, cinsel tercih etme, siber zorbalık, yasadışı içerik ihlali vb. Gibi çevrimiçi güvenlik (e-Güvenlik) endişelerini bildirme prosedürü hakkında bilgilendirilecektir.
- Belirlenmiş Koruyucu Tedbirler (DSL), daha sonra oluşabilecek çocuk koruma endişelerini içeren herhangi bir çevrimiçi güvenlik (e-Güvenlik) olayı hakkında bilgilendirilecektir.
- İnternet'in yanlış kullanımı ile ilgili şikayetler, okulun şikayet 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 müdüre yönlendirilecektir.

- Okul şikayet prosedürü öğrencilere, velilere ve personele bildirilecektir.
- Şikayet ve ihbar prosedürü personele bildirilecektir.
- Okul topluluğunun tüm üyeleri, gizliliğin öneminden ve endişeleri bildirmek için resmi okul usullerine uyma gereğinden haberdar olmalıdırlar.
- Okul topluluğunun tüm üyeleri, çevrimiçi ortamda güvenli ve uygun davranış hakkında uyarılacak ve okul camiasının herhangi bir diğer üyesine zarar vermek, sıkıntı yaşatmak veya suç oluşturan herhangi bir içerik, yorum, resim veya video yayımlamamanın önemini hatırlatılacaktır.
- Okul, çevrimiçi güvenlik (e-Güvenlik) olaylarını, gerektiği yerde, okul disiplini / davranış politikasına uygun olarak yönetir.
- Okul, ebeveynleri / bakıcıları, ihtiyaç duyulduğunda belirli endişelerle ilgili bilgilendirir.
- Herhangi bir soruşturma tamamlandıktan sonra okul öğrenilen dersleri belirleyecek, derslerle ilgili bilgi alacak ve değişiklikleri gerektiği gibi uygulayacaktır.
- Sorunları çözmek için ebeveynlerin ve çocukların okulla ortak çalışması gerekmektedir.

2019-2020 1.DÖNEM ÖĞRETMENLER KURULU TOPLANTISI GÜNDEM MADDELERİ:

1 e-Güvenlik Politikası

2019-2020 1.DÖNEM ÖĞRETMENLER KURULU TOPLANTISI GÜNDEM MADDELERİ:

7.MADDE: A-) E-GÜVENLİK : ÖĞRENCİLERİN, VELİLERİN, ÖĞRETMENLERİN VE TÜM OKUL PERSONELİNİN E-GÜVENLİK KONUSUNDA BİLGİLENDİRİLMESİ:

1-Okulumuz 2019-2020 1. Dönem Öğretmenler Kurul toplantısında E-güvenlik konusu öncelikli gündem maddeleri içerisinde görüşülmüştür. Okulumuz E- Güvenlik Politikası gereğince alınan

kararlar;

1-Okul idaresinin belirleyeceği yer, zaman ve tarihlerde tüm öğretmenlere ve okul personeline, şube bazında tüm öğrencilere Bilişim Öğretmenimiz ve Rehberlik Servisinin içeriklerini işbirliği içinde hazırlayacağı e-Güvenlik seminerleri verilmesine ve tüm hedef kitlelerinin katılımlarının sağlanması için gerekli çalışmaların ortaklaşa yapılmasına karar verilmiştir.

2-Öğretmenlerimizin bireysel araştırma yapmaları, Eba'da online kurslara katılmalarına, kazanımların zümre ve öğretmenler toplantılarında paylaşmalarına karar verilmiştir.

3-Öğretmenlerimizin bu çalışmalarının;

İnternet teknolojisi ile ilgili temel kavram ve terimler

İnternetin günlük hayattaki yeri ve kullanımı

İnternet ortamında bilgiye hızlı ve etkin ulaşma yöntemleri

Güvenilir web kaynağı kriterleri

Dijital yurttaşlık kuralları

Dijital ayak izi ve çevrim içi itibar yönetimi

Güçlü parola üretme yöntemleri

Çevrim içi karşılaşabileceğimiz siber tuzaklardan korunma,

Sanal Zorbalık Tanımı,Siber Zorbalığın Görülme Biçimleri,Geleneksel zorbalık ve Sanal Zorbalık Farkı, Sanal Zorbalığın Yaygınlığı,Sanal Zorbalığın Nedenleri,Sanal Zorbalığın Sonuçları,Sanal Zorbalıkla Başa Çıkma ve Korunma konularını içermesine böylelikle;

sınıflarda eğitim-öğretim faaliyetlerini oluşturan internet tabanlı-proje tabanlı bireysel veya gurup çalışmasını gerektiren proje ve günlük ödevlerde, ayrıca ders dışı sosyal kullanım alanlarında çevrim içiyken güvenli olmalarına, etik davranışlar geliştirmelerine ve dijital yurttaşlık kurallarını önemseyen, internet kullanıcıları olmalarını sağlamalarına karar verilmiştir.

-Her yıl Şubat ayında kutlanan Güvenli İnternet Günü'nün çeşitli aktivitelere yer verilerek kutlanmasına karar verilmiştir.

2-Okulunuzda taşınabilir cihazların/cep telefonlarının kullanımı hakkında bir politika var mıdır?

7.MADDE: B-) ÖĞRENCİLERİN TAŞINILABİLİR CİHAZLARINI VE CEP TELEFONLARINI OKULA GETİRMELERİ

1-Okulumuz E-Güvenlik Politikası gereğince öğrencilerimizin taşınabilir cihazlarını veya telefonlarını okula getirmeleri ve kullanmalarına izin verilmeyeceği / yasaklanması kabul edilmiş, veli toplantılarında konu ile ilgili velilerin tekrar bilgilendirilmesi, öğrencilerine evden okula gelirken telefon tablet gibi cihazlarını vermemelerini, sadece acil durumlarda Okul İdaresine haber verilerek okul saatleri içerisinde okul idaresinde veya sınıf öğretmenlerinde kalacak şekilde okula getirmeleri, (okul saati sona erdikten sonra teslim edilmesi) sınıflarda yapılacak düzenli kontrollerle bunun engellenmesine karar verilmiştir.

2-Ailelerin ve öğrencilerin bireysel görüşmelerle kuralların hatırlatılmasına rağmen, bu kurallara karşı çıkılması, ısrarla devam edilmesi ve özellikle eğitim öğretim faaliyetleri amaçlarının dışında kullanılmasının ispatlandığı durumda yapılacak toplantılarla yeni tedbirler alınmasına karar verilmiştir.

3-Öğretmenlerin sınıf içi uygulamalarıyla ilgili ve ihtiyaç duyduğu konularda sadece güvenli eğitim sitelerini ziyaret etmelerine karar verilmiştir

4-Okul politikalarınız; öğrencilerinizin, velilerinizin ve okul personelinin fotoğraflarının çekilmesi ve onların okulda fotoğraf çekmesi ve yayınlanmasına ilişkin bir bölüm içeriyor mu

2019-2020 1.DÖNEM ÖĞRETMENLER KURULU TOPLANTISI GÜNDEM MADDELERİ:

7.MADDE: C-) ÖĞRENCİLERİN, VELİLERİN, VE OKUL PERSONELİNİN FOTOĞRAFLARININ ÇEKİLMESİ VE OKULDA FOTOĞRAF ÇEKİP YAYINLAMASI;

-Tüm öğretmenlerin öğrencilerin velilerinden ve yasal varislerinden okulumuzda kutlanan belirtili gün ve haftalarda, milli ve dini kutlama programlarında, E-twinning projelerinde, okulumuzu tanıtan ve yapılan aktivitileri (spor, resim, müzik, Tubitak, Avrupa Birliği Erasmus+ projeleri, gezi ve kültürel aktiviteler) içeren haber kaynaklarında ve videolarda kullanılmak üzere çekilen fotoğrafların kullanılması için izin belgesi alınmasına,

-Çekilen fotoğraflarda ve videolarda Milli Eğitim Bakanlığımızın 2017-12 Genelgesi gereğince öğrencilerin yüzlerinin uzaktan ve belirgin olmadan çekilmesine, ses kayıtları içermeyeceğine,

-Velilerin belirtilen aktivitelerde (okul sınırları içerisinde) sadece kendi öğrencilerinin fotoğraflarını çekebileceklerini ve online platformlarda diğer öğrencilerin fotoğraflarını paylaşamayacaklarını içeren bir yazı ile bilgilendirilmelerine,

-Öğretmenlerimizden okulumuzda kutlanan belirtili gün ve haftalarda, milli ve dini kutlama programlarında, E-twinning projelerinde, okulumuzu tanıtan ve yapılan aktivitileri (spor, resim, müzik, Tubitak, Avrupa Birliği Erasmus+ projeleri, gezi ve kültürel aktiviteler) içeren haber kaynaklarında ve videolarda kullanılmak üzere çekilen fotoğraflarının kullanılması için izin belgesi alınmasına,

-Öğretmenlerimizden; öğrencilerin isimlerini, yaşlarını veya diğer kişisel bilgilerini , resimlerini, okulumuzda kutlanan belirtili gün ve haftalarda, milli ve dini kutlama programlarında, E-twinning projelerinde, okulumuzu tanıtan ve yapılan aktivitileri (spor, resim, müzik, Tubitak, Avrupa Birliği Erasmus+ projeleri, gezi ve kültürel aktiviteler) içeren haber kaynaklarında ve videoların dışında kendi web sitelerinde ve sosyal paylaşım sitelerinde yayınlamayacaklarına dair taahhütname alınmasına karar verilmiştir.

OLCAY AKDEMİR COŞKUN

OKUL MÜDÜR VEKİLİ

11.09.2019