E-Güvenlik

Çağlayan Şehit İsmail Dinç Ortaokulu e-Güvenlik Politikası ve Amaçları

- Çağlayan Şehit İsmail Dinç Ortaokulu, çevrimiçi güvenliğin(e-Güvenlik) bilgisayarlar,tabletler,cep telefonları veyaoyunkonsolları gibiteknolojiyi kullanırken, dijital dünyadaki çocukların ve yetişkinlerin korunması için vazgeçilmez bir unsur olduğuna inanmaktadır.
- Çağlayan Şehit İsmail Dinç Ortaokulu, internetin ve bilgi iletişim teknolojilerinin günlük yaşamın önemli bir parçası olduğunu belirtir.Dolayısıyla,riskleri yönetmek ve bunlara tepki vermek için,

stratejiler geliştirmenin yollarını öğrenmek ve çevrimiçi ortamda esneklik kazanmak için, güç sahibi olmak için çocuklar desteklenmelidir.

- Çağlayan Şehit İsmail Dinç Ortaokulu, eğitim standartlarını yükseltmek, başarıyı teşvik etmek, personelin mesleki çalışmalarını desteklemek ve yönetim işlevlerini geliştirmek için toplumun kaliteli İnternet erişimi sunma yükümlülüğüne sahiptir.
- Çağlayan Şehit İsmail Dinç Ortaokulu, tüm çocukların ve personelin çevrimiçi olarak potansiyelzararlardan korunmasını sağlamakla sorumludur.

Çağlayan Şehit İsmail Dinç Ortaokulu çevrimiçi e-Güvenlik Politikasının amacı şudur:

- Çağlayan Şehit İsmail Dinç Ortaokulu güvenlivegüvenlibirortamolduğundaneminolmakiçin, toplumun tüm üyelerinden beklenen ana ilkeleri, güvenli ve sorumlu kullanımteknolojisi ile ilgili olarak tanımlamak.
- Çağlayan Şehit İsmail Dinç Ortaokulu topluluğunun tüm üyelerini çevrimiçi olarak korumak vegüvenliğini sağlamak.
- Teknolojinin potansiyel riskleri ve yararları konusunda Çağlayan Şehit İsmail Dinç Ortaokulutopluluğunun tüm üyelerinde farkındalık yaratmak.
- Tüm personelin güvenli ve sorumlu bir şekilde çalışmasını sağlamak, olumlu davranışları online olarak modellemek ve teknolojiyi kullanırken kendi standartlarını ve uygulamalarını yönetme gereksiniminin farkında olmak.
- Okuldaki tüm üyeler tarafından bilinen çevrimiçi güvenlik endişelerine yanıt verirken açıkça kullanılacak prosedürleri tanımlamak.

- Bu politika, yönetim organı, öğretmenler, destek personeli, harici yükleniciler, ziyaretçiler, gönüllülerveokuladınahizmet verenveyabunları yerinegetirendiğerkişiler(topluolarak bu politikada 'personel' olarak anılacaktır) dâhil olmak üzere tüm personel için geçerlidir. Bununyanı sıra: Bu politika,internet erişimi ve kişisel cihazlar da dâhil olmak üzere bilgi iletişim cihazlarının kullanımı için geçerlidir; çocuklar, personel ya da diğer kişilere, çalıştıkları dizüstü bilgisayarlar,tabletler veya mobil cihazlar gibi uzaktan kullanım için de geçerlidir.

Çevrimiçi Güvenlik Politikası yazma ve gözden geçirme:

- Çağlayan Şehit İsmail Dinç Ortaokulu Online güvenlik politikası, personel, öğrenciler ve ebeveynleri içeren,gerektiğinde uzman tavsiyesi vekatkısı ile okul tarafından yazılmıştır.
- Politika, okul yönetimi tarafından onaylandı ve kabul edildi.

- Okul yönetimi çevrimiçi güvenlik sorumlusu olarak Bilişim Teknolojileri Öğretmeni Yılmaz KAYA'yı atadı.
- Okul,onlinegüvenlik(e-Güvenlik) içinsorumluluğuüstlenmeküzereokulyönetim kurulu üyesi olarak Müdür Yardımcısı Hasan DURNA atandı.

- Çevrimiçi güvenlik(e-Güvenlik) Politikası ve uygulaması,en az yılda bir kez veya gerekirse daha erken bir tarihte Çağlayan Şehit İsmail Dinç Ortaokulu tarafından gözden geçirilecektir.

1.1 Topluluk için kilit sorumluluklar

1.1.1 Okul/belirlemeyönetimiveliderlikekibinin başlıcasorumlulukları şunlardır:

- Çevrimiçi güvenlik vizyonunu ve kültürünü, okul topluluğu boyunca uygun destek ve istişarede bulunarak ulusal ve yerel tavsiyeler doğrultusunda tüm paydaşlara geliştirmek, sahip olmak ve bunları teşvik etmek.
- Çevrimiçi güvenliğin tüm toplum tarafından bir korunma meselesi olarak görülmesini ve güçlü bir çevrimiçi güvenlik kültürünü proaktif olarak geliştirilmesini sağlamak.
- Onlarınçevrimiçi güvenlik rolü ve sorumluluklarını yerinegetirmekiçinyeterlizamanve kaynağa sahip olmalarını sağlayarak Belirlenmiş Koruyucu Liderin (DSL) desteklenmesi.
- Çevrimiçi güvenlikle ilgili uygun profesyonel davranışı ve teknolojinin kullanımını kapsayan Kabul Edilebilir Kullanım Politikasını da içeren 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 uygunve uygun filtreleme ve izleme sistemlerinin kurulmasını sağlamak.
- Okulun / ortam sistemlerinin ve ağlarının güvenliğini ve güvenliğini izlemek ve okul / ortam 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 veuygun güvenli iletişimle ilgili rehberlik sağlanması.
- Çevrimiçi güvenliğin tüm öğrencilere çevrimiçi güvenliği, ilgili riskleri ve güvenli davranışları yaşauygunbir şekilde anlamasını sağlayan ilerici birbütünokul/ öğretim müfredatı içerisinde yer almasını sağlama.
- Çevrimiçi güvenlik olaylarından haberdar olmak ve dış kurumların ve desteğin uygun şekilde irtibatlandırılmasını sağlamak.
- Çevrimiçi korunma kayıtlarını almak ve düzenli olarak gözden geçirmek ve bunları gelecekteki uygulamaları bilgilendirmek ve şekillendirmek için kullanmak.
- Okul, yerel ve ulusal destek dâhilolmaküzere çevrimiçigüvenlik endişeleri ile ilgili olarak erişmek için okul /çevre topluluğu için sağlam raporlama kanallarının bulunmasını sağlamak.
- Cihazların güvenli ve sorumlu kullanılmasını sağlamak da dâhil olmak üzere, teknolojinin güvenli kullanımı ile ilgili uygun risk değerlendirmelerinin yapılmasını sağlamak.
- Yönetim organının üyesi olan çevrimiçi güvenliğin sağlanmasına ilişkin sorumluluk üstlenecek bir kişinin sağlanması.
- İyileştirme güç ve alanlarını belirlemek için mevcut çevrimiçi güvenlik uygulamasını denetlemek ve değerlendirmek.
- Belirlenmiş KoruyucuLiderin(DSL),çevrimiçigüvenliksorumlusuilebirlikteçalışmasını sağlamak.

1.1.2 Belirlenmiş Koruyucu Liderin temel sorumlulukları şunlardır:

- Tüm çevrimiçi korunma konularında adlandırılmış bir irtibat noktası olarak hareket etmek ve diğer personel üyeleri ve diğer ajanslarlauygun şekilde iletişime geçmek.
- Çevrimiçigüvenlikle ilgili mevcut araştırma, mevzuat veeğilimlerle güncel 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 ve daha geniş topluluğa tanıtılmasını sağlamak
- Çevrimiçi güvenlik olaylarının ve kayıt yapılarını ve mekanizmalarını koruyan okulların bir parçası olarak alınan önlemlerin kayıtlarını tutmak.
- Okul yönetim ekibine ve diğer birimlere, çevrimiçi güvenlik sorunları ve yerel veriler / rakamlar hakkında raporvermek.
- Yerel ve ulusal kurumlarla irtibat kurmak.
- Paydaş katkısı ile düzenli olarak çevrimiçi güvenlik politikalarını, Kabul Edilebilir Kullanım Politikalarını (AUP'ler) ve diğerilgili politikaları gözdengeçirmek ve güncellemek içinokul/ liderlik ve yönetimle birlikte çalışmak.
- Çevrimiçigüvenliğindiğeruygunokulpolitikalarıveprosedürleriyle bütünleştirilmesini sağlamak.

1.1.3 Tüm çalışanların kilit sorumlulukları şunlardır:

- Çevrimiçi güvenlik politikalarının geliştirilmesine katkıda bulunmak.
- Kabul Edilebilir Kullanım Politikalarını (AUP'lar) okumakveonlara bağlı kalmak.
- Okul / ortam sistemlerinin ve verilerin güvenliğinden sorumlu olmak.
- Bir dizi farklı çevrim içi güvenlik konusundaki farkındalığa sahip olmak ve onların bakımında çocuklarla nasıl ilişkili olabileceklerini bilmek.
- Yenive gelişmekte olan teknolojiler kullanıldığında iyi uygulamaları modelleme
- Mümkün olduğunca müfredat ile çevrimiçi güvenlik eğitimini ilişkilendirme.
- Okulkoruma politikalarını ve prosedürlerini takipederek endişe duyan bireylerin belirlenmesi ve uygun önlem alınması.
- Çevrimiçi güvenlik konusunu ne zaman ve ne kadar içtevedışta tırmanacağınızı bilmek.
- Çevrimiçi güvenlik konularda, dâhilive hariciolarak, uygun desteğin işaretinikoymak.
- Kişisel ve kişisel teknoloji kullanımlarında, hem açık hem de kapalı alanda profesyonel bir davranış seviyesinin korunması.
- Olumlu öğrenme fırsatlarına vurgu yapmak.
- Bu alanda mesleki gelişim için kişisel sorumluluk almak.

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

- Öğrenme fırsatlarının hala en üst düzeye çıkartılmasını sağlarken güvenli online uygulamalarını destekleyen güvenli ve güvenli bir teknik alt yapının sağlanması.
- Liderlik ve 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 DSLile paylaşılması.
- Okulun ağının düzenli olarak izlenmesini sağlamak ve kasıtlı yada yanlışlıkla yapılan yanlış kullanımı DSL'ye bildirmek.
- Herhangi bir ihlal veya sorunu DSL ve liderlik ekibine rapor etmek ve birlikte kaydedilmesini ve uygun önlemlerin tavsiye edildiği şekilde alınmasını sağlamak.
- Teknikalt yapınıngüvenliğivegüvenliğiileilgiliolarakilgilimevzuathakkındabiranlayış geliştirilmesi.
- Herhangi bir ihlali bildirin ve yerel otorite (veya diğer yerel veya ulusal kurumlar) ile teknik altyapı konularında irtibat kurmak.
- Özellikle uygunçevrimiçigüvenlikpolitikalarıveprosedürlerinin geliştirilmesi ve uygulanmasında DSL ve liderlik ekibine teknik destek sağlamak.
- Okulun BİT altyapısının / sisteminin güvenli olduğunu ve kötüye kullanım veyakötüniyetli saldırılara açık olmamasını sağlamak.
- Tümortammakinelerinde ve taşınabiliraygıtlarda uygunanti-virüsyazılımının ve sistem güncellemelerinin kurulmasını sağlamak.
- Uygun olan güçlü parolaların en genç kullanıcıları hariç olmak üzere tümüne uygulandığından emin olmak.

1.1.5 Çocukların ve gençlerin başlıca sorumlulukları şunlardır:

- Çevrimiçi güvenlik politikalarının geliştirilmesine katkıda bulunmak.
- Okulun Kabul EdilebilirKullanım Politikalarını(AUP'lar) okumakveonlarabağlıkalmak.
- Çevrim içi ve çevrimdışı başkalarının hislerine ve haklarına saygı duymak.
- İşler tersgiderse, güvenilir biryetişkinden yardımistemek ve çevrimiçigüvenlik sorunlarıyla karşılaşan diğer kişileri desteklemek.

Bireysel yaşlarına, yeteneklerine ve zayıf yönlerine uygun bir seviyede:

- Kendilerini ve başkalarını çevrimiçi olarak korumak için sorumluluk almak.
- Yeni ve gelişmekte olan teknolojilerin getirdiği fırsatlar ve risklerle ilgili olarak kendi bilinci ve öğrenimlerinden sorumlu olmak.
- Bellibir teknolojiyi kullanmanın kişisel risklerini değerlendirmek ve bu riskleri sınırlamak için güvenli ve sorumluluk sahibi davranmak.

1.1.6 Ebeveynlerin başlıca sorumlulukları şunlardır:

- Okul Kabul Edilebilir Kullanım Politikalarını okumak, çocuklarını bu politikaya bağlı kalmaya teşvik etmek ve uygun olduğunca kendilerinin de bağlı kalmasını sağlamak.
- Çocuklarıyla çevrimiçi güvenlik konularını tartışmak, okulun çevrimiçi güvenlik Yaklaşımlarını desteklemek ve evde uygun güvenli çevrimiçi davranışları pekiştirmek.
- Teknoloji ve sosyal medyanın güvenli ve uygun kullanımını modellemek.
- Davranışlarında, çocuğun çevrimiçi olarak zarar görme tehlikesi altında olduğunu gösteren değişiklikleri belirlemek.
- Okulveyadiğeruygunkurumlardan, kendileri ve yaçocukları çevrimiçiproblemveya sorunlarla karşılaşırsa yardım veya destek istemek.

- Okulun çevrimiçi güvenlik politikalarının oluşturulmasına katkıda bulunmak.
- Öğrenme platformları ve diğer ağ kaynakları gibiokulsistemlerinigüvenli ve uygunbir şekilde kullanmak.
- Yeni ve gelişmekte olan teknolojilerin getirdiği fırsatlar ve risklerle ilgili olarak kendi bilinci ve öğrenimlerinden sorumlu olmak.

Çevrimiçi İletişim ve Teknolojinin Daha Güvenli Kullanımı:

1.1 Okul/ web sitesinin yönetilmesi

- Web sitesinde iletişim bilgileri okul adresi, e-postave telefon numarası olacaktır. Personel veya öğrencilerin kişisel bilgileri yayınlanmayacaktır.
- Okul Müdürü yayınlanan çevrimiçiiçerikiçingenelyayınsorumluluğunu alacakvebilgilerin doğru ve uygun olmasını sağlayacaktır.
- Web sitesi, erişilebilirlik fikri mülkiyet haklarına saygı, gizlilik politikaları ve telif hakkı da dâhil olmak üzere okulun yayın yönergelerine uyacaktır.
- Spammaillerden korunmak için e-postaadresleri çevrimiçiolarakdikkatlibir şekilde yayınlanacaktır.
- Öğrenci çalışmaları öğrencilerin izniyle yada ebeveynlerinin izniyle yayınlanacaktır.
- Okulwebsitesininyöneticihesabı, uygunbir şekilde güçlü şifreyle şifrelenerek korunacaktır.
- Okul, çevrimiçi güvenlik dâhil olmak üzere, toplumun üyeleri için okul web sitesinde korunma hakkında bilgi gönderecektir.

1.2 Çevrimiçi görüntü ve videolar yayınlama:

- Okul, çevrimiçi paylaşılan tüm resimlerin ve videoların okul resim kullanımı politikasına uygun şekilde kullanılmasını sağlayacaktır.
- Okul, resimlerin ve videoların tümünün, veri güvenliği, Kabul Edilebilir Kullanım Politikaları, Davranış Kuralları, sosyal medya, kişisel cihazların ve cep telefonlarının kullanımı gibi diğer politikalar ve prosedürlere uygun şekilde yer almasını sağlayacaktır.
- Görüntü politikasına uygun olarak, öğrencilerin resimlerinin / videolarının elektronik olarak yayınlanmasından önce her zaman ebeveynlerin yazılı izni alınacaktır.

1.3 Eğitim amaçlı resmi video konferans ve web kamerası kullanımı:

- Okul, videokonferansın çok çeşitli öğrenme avantajlarıyla zorlubirfaaliyet olduğunu kabul eder. Hazırlık ve değerlendirme, tüm faaliyet için gereklidir.
- Tüm video konferans ekipmanları, kullanılmadığında ve uygun olduğunda kapatılacaktır, otomatik cevaplamaya ayarlanmayacaktır.
- Harici IP adresleri diğer sitelere sunulmayacaktır.
- Video konferans iletişim detayları kamuoyuna açık olarak paylaşılmayacaktır.
- Video konferans ekipmanları güvenli bir şekilde tutulacak ve gerekirse kullanılmadığında kilitlenecektir.
- Okul video konferans ekipmanları izinsiz olarakokul binalarından çıkarılmayacaktır.
- 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 güvenlive gizli olmasını sağlayacaktır.

Kullanıcılar:

- Öğrenciler, birvideokonferansaramasıveyamesajıhazırlamadanveyacevaplamadanöncebir öğretmeninden izin isteyecektir.
- Video konferans, öğrencilerin yaşı ve yeteneği için uygun bir şekilde denetlenecek.
- Velilerin rızası,çocuklar video konferans faaliyetlerine katılmadan önce alınacaktır.
- Video konferans, sağlam bir risk değerlendirmesini takiben, resmi ve onaylanmış iletişim kanalları vasıtasıyla gerçekleşecektir
- Sadece ana yöneticilere video konferans yönetim alanlarına veya uzaktan kumanda sayfalarına erişim hakkı verilecektir.
- Eğitimselvideokonferansservisleriiçinözeloturumaçma ve şifre bilgileriyalnızca personellere verilecek ve gizli tutulacak.

İçerik:

- Bir video konferans dersi kaydederken, tüm siteler ve katılımcılar tarafından yazılı izin alınacaktır. Konferansın başlangıcında kayıt nedeni belirtilmeli ve video konferans kaydı tüm taraflaraaçıkolmalıdır. Kaydedilenmalzemelergüvenlibirşekilde saklanacaktır.
- Üçüncütarafmateryalleridâhiledilecekse, okulüçüncüşahsınfikrimülkiyethaklarınıihlal etmektenkaçınmakiçinbukaydınkabuledilebilirolupolmadığınıkontroledecektir.
- Okul,birvideokonferansakatılmadanöncediğerkonferanskatılımcılarıyladiyalog kuracak. Okuldeğilse, okul sınıfiçinuygunolanmateryaliteslimaldığınıkontroledecektir.

1.4 İnternetin ve ilgili cihazların uygun ve güvenli derslik kullanımı:

- İnternet kullanımı eğitimsel erişimin önemli bir özelliğidir ve tüm çocuklar bütünleşik okul müfredatının bir parçası olarak sorunlarını yanıtlamak için stratejiler geliştirmelerini destekleyecek ve onlara yardımcı olacak yaşa ve yeteneğe uygun eğitim alacaklardır. Okulun/ ortamın internet erişimi eğitimi geliştirmek ve genişletmek için tasarlanacaktır.
- İnternet erişim seviyeleri müfredat gerekliliklerini ve öğrencilerin yaş ve yeteneklerini yansıtacak şekilde gözden geçirilecektir.
- Çalışanların tüm üyeleri, çocukları korumak için tek başına filtrelemeye güvenmeyeceklerinin farkındadır. Gözetim, sınıf yönetimi, güvenli ve sorumlu kullanım eğitimi önemlidir.

Öğrencilerin yaşlarına ve yeteneklerine uygun olacaktır:

- Genç öğrencilerin İnternet'e erişimi, yetişkinlerin gösteri yaparak, öğrencilerin yaşı ve yeteneği için planlanan öğrenme çıktılarını destekleyen belirli ve onaylanmış çevrimiçi materyallere doğrudan denetlenen erişimle sağlanacaktır.
- 11-14 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 uygun bir şekilde gözetim altına alınacaklardır.

- Tüm okula ait cihazlar, okulun Kabul Edilebilir Kullanım Politikasına uygun olarak ve uygun güvenlik ve güvenlik önlemleri alınarak kullanılacaktır.
- Personel üyeleri, web sitelerini, araçlarını ve uygulamalarını sınıfta kullanmadan önce veya evde kullanmayı önerirken daima değerlendirecektir.
- Öğrenciler, bilginin konumlanması, alınması ve değerlendirilmesi becerileri de dâhil olmak üzere, İnternette araştırmada etkili kullanımı konusunda eğitilecektir.
- Okul, personelin ve öğrencilerin İnternet'ten türetilen materyallerin telif hakkı yasalarına uygun olmasını ve bilgi kaynaklarını kabul etmesini sağlayacaktır.
- Öğrencilere, okuduklarıveyagösterilen bilgilerindoğruluğunukabuletmedenönce eleştirel düşünmeleri öğretilecektir.
- Çevrimiçimateryallerindeğerlendirilmesi, herkonudaöğretme veöğrenmenin bir parçasıdır ve müfredatta bir bütün olarak görülür.
- Okul, öğrencileri ve çalışanlarımızın güvenli ve gizli bir ortamda iletişim kurmalarını ve işbirliği yapmalarını sağlamak için interneti kullanacaklardır.

2. Kişisel Cihazların ve Cep Telefonlarının Kullanımı

2.1 Kişisel cihazlar ve cep telefonları ile ilgili gerekçe:

- Cep telefonlarının ve çocukların, gençlerin ve yetişkinler arasındaki diğer kişisel cihazların yaygın bir şekilde sahiplenilmesi, tüm üyelerin Çağlayan Şehit İsmail Dinç Ortaokulu topluluğunun cep telefonlarının ve kişisel cihazların sorumlu bir şekilde kullanılmasını sağlamak için gerekli adımları atmalarını gerektirir.
- Çocukların,gençlerin ve yetişkinlerin cep telefonlarının ve diğer kişisel cihazların kullanımı, okul tarafından kararlaştırılacak ve okul Kabul Edilebilir Kullanım veya Cep Telefonu Politikası dâhil olmak üzere uygun politikalarda yer alacaktır.
- Çağlayan Şehit İsmail Dinç Ortaokulu, mobilteknolojilerle yapılan kişisel iletişimin, çocuklar, personel veanne-babalar için gündelik yaşamın kabul edilen bir parçası olduğunun farkındadır; ancak bu türteknolojilerin okulda güvenlive uygun bir şekilde kullanılmasını gerektirir.

3. Kişisel cihazların ve cep telefonlarının güvenli bir şekilde kullanılması için beklentiler:

- Kişisel cihazların ve cep telefonlarının kullanımı yasaya ve diğer uygun okul politikalarına uygun olarak yerine getirilecektir.
- Sahaya getirilen her türlü elektronik cihazın sorumluluğu kullanıcıya aittir. Okul, bu tür öğelerin kaybı, çalınması veya zarar görmesi konusunda sorumluluk kabul etmez. Okul, bu tür cihazların potansiyel veya fiili neden olduğu olumsuz sağlık etkileri için sorumluluk kabul etmez.
- Kötüye kullanım veya uygun olmayan mesajların veya içeriğin cep telefonları veya kişisel cihazlarla gönderilmesi, topluluğun herhangi bir üyesi tarafından yasaklanır ve herhangi bir ihlal, disiplin / davranış politikasının bir parçası olarak ele alınacaktır.
- Çağlayan Şehit İsmail Dinç Ortaokulu topluluğunun tüm üyelerine cep telefonlarını veya cihazlarını kayıp,hırsızlık veya hasardan korumak için adımatmaları önerilir.
- Çağlayan Şehit İsmail Dinç Ortaokulu topluluğunun tüm üyelerinden, kayboldukları veya çalındığı takdirdeyetkisizaramalarınveyahareketlerintelefonlarındaveyacihazlarında yapılamayacağından emin olmak için şifreler / pin numaraları kullanmaları

önerilir. Parolalarvepinnumaralarıgizlitutulmalıdır. Ceptelefonları ve kişisel cihazlar paylaşılmamalıdır.

- Çağlayan Şehit İsmail Dinç Ortaokulu topluluğunun tüm üyelerine, cep telefonlarının ve kişiselcihazlarının saldırgan, küçümseyen veya başka şekilde okul/ayar politikalarına aykırı düşen herhangi bir içerik içermediğinden emin olmaları önerilir.

3.1 Öğrencilerin kişisel cihazlarını ve cep telefonlarını kullanımı:

- Öğrenciler, kişiselcihazlarınveceptelefonlarınıngüvenliveuygunkullanımıkonusunda eğitim alacaklardır.
- Çocuklarınceptelefonlarının ve kişisel cihazlarıntümkullanımları, kabuledilebilirkullanım politikasına uygun olarak gerçekleşecektir.
- Cep telefonları veya kişisel cihazlar, öğrencilerin bir öğretim üyesinin onayını alarak onaylanmışveyönlendirilmişmüfredattabanlıetkinlikkapsamındaolmadıklarısürece dersler veya resmi okul saatlerinde öğrenciler tarafından kullanılamaz.
- Çocukların cep telefonlarını veya kişisel cihazlarını eğitim etkinliğinde kullanımı, okul idaresi tarafından onaylandığında gerçekleşecektir.
- Bir öğrenci ebeveynlerini arama gereği duyduğunda, okul telefonunu kullanmasına izin verilecektir.
- Ebeveynlerinokulsaatlerindeceptelefonuyla çocuklarıylailetişimkurmamaları, okul idaresine başvurmaları önerilir. İstisnai durumlarda öğretmenin onayladığı şekilde istisnalara izin verilebilir.
- Öğrenciler, telefon numaralarını yalnızca güvenilir arkadaşlarına ve aile üyelerine vermelidirler.
- Öğrencilere, cep telefonlarının ve kişisel cihazların güvenli ve uygun bir şekilde kullanımı öğretilecek ve sınırların ve sonuçların farkına varılacaktır.
- Öğrencininkişiselcihazındaveyaceptelefonundabulunanmateryalinyasadışıolabileceği veya cezai birsuçla ilgili kanıtsağlayabileceğinden şüpheleniliyorsa, cihazdahaayrıntılı araştırma için polise teslim edilir.

3.2 Kişisel cihazların ve cep telefonlarının personel kullanımı:

- Personelin, kendikişisel telefonlarınıveyacihazlarını, çocukların, gençlerin ve ailelerinin, mesleki bir kapasitede, ortamın içinde veya dışındaki bölgeleriyle bağlantı kurmalarına izin verilmez. Bu konuyu tehlikeye atacak önceden var olan ilişkiler yöneticilerle görüşülecektir.
- Personel,çocukların fotoğraflarını veya videolarını çekmek için cep telefonları,tabletler Veya kameralar gibi kişisel cihazları kullanmaz ve yalnızca bu amaçla işle sağlanan ekipmanı kullanır.
- Personel her hangi bir kişisel cihazı doğrudan çocuklarla kullanmaz ve ders/ eğitim etkinlikleri sırasında yalnızca okul tarafından sağlanan ekipmanı kullanır.
- Personel, kişisel telefonların ve cihazlarınherhangi bir şekilde kullanımının daimaveri koruma veilgiliokulpolitikası veprosedürleri uyarıncayerinegetirilmesinisağlayacaktır
- Personelkişiselceptelefonlarıvecihazları derssaatlerindekapatılıp/sessizmodageçirilir.
- Bluetooth veya diğer iletişim biçimleri ders saatlerinde "gizlenmiş" veya kapalı olmalıdır.
- Acil durumlarda okul idaresi tarafından izin verilmemişse, kişisel cep telefonları veya cihazları öğretim dönemleri boyunca kullanılamaz.

- Personel, cep telefonları ve kişisel cihazlar üzerinden sitede satın alınan içeriğin profesyonel rolü ve beklentileri ile uyumlu olmasını sağlayacaktır.
- Bir personel okul politikasını ihlal ettiği durumlarda disiplin işlemi yapılır.
- Bir personelin, bir cep telefonuna veya kişisel bir cihaza kaydedilen veya saklanan yasadışı içeriğe sahip olduğu veya ceza gerektiren bir suç işlemiş olması durumunda, polise ulaşılacaktır.
- Personelin cep telefonunu veya cihazlarını kişisel olarak kullanmalarını içeren herhangi bir iddiaya okul yönetim politikasını izleyerek yanıt verilecektir.

3.3 Ziyaretçilerkişiselcihazlarınveceptelefonlarınınkullanılması:

- Ebeveynlerveziyaretçiler, okulunkabuledilebilirkullanımpolitikasınauygunolarakcep telefonlarını ve kişisel cihazları kullanmalıdır.
- Fotoğraflar veya videolar çekmek için ziyaretçiler ve ebeveynler tarafından cep telefonlarının veya kişisel cihazların kullanılması, okul resim kullanımı politikasına uygun olarak gerçekleştirilmelidir.
- Okul, ziyaretçilere kullanım beklentilerinibildirmek içinuyguntabela ve bilgileri sağlayacak ve sunacaktır.
- Personelinuygunvegüvenliolduğundasorunlarakarşıçıkmasıbeklenirveherzaman ziyaretçilerin herhangi bir ihlalini idareye bildirecektir.

4 . Politika Kararları

4.1 Çevrimiçi riskleri azaltmak:

- Çağlayan Şehit İsmail Dinç Ortaokulu internetin yeni uygulamalar, araçlar, cihazlar, siteler vemateryallerin hızla geliştiği sürekli değişen bir ortam olduğunun farkındadır.
- Gelişen teknolojiler eğitimsel fayda açısından incelenecek ve okul liderliği ekibi, okulda kullanılmasınaizinverilmedenönceuygunriskdeğerlendirmelerininyapılmasını sağlayacaktır
- Okul, personelinveöğrencilerinuygunolmayanveyayasadışıiçeriğeerişmesiniönlemek için uygun filtreleme ve izleme sistemlerinin kurulmasını sağlayacaktır.

- Okul, kullanıcıların yalnızca uygun materyallere erişmesini sağlamak için makul önlemleri alacaktır. Bununla birlikte, internet içeriğinin küresel ve bağlanmış niteliğinden dolayı, uygun olmayan materyallerin bir okul/bilgisayar yada cihaz vasıtasıyla hiçbir zaman gerçekleşmeyeceğini garanti etmek her zaman mümkün değildir.
- Okul, çevrimiçigüvenlik(e-Güvenlik) politikasınınyeterliolupolmadığını vepolitikanın uygulanmasının uygun olup olmadığını belirlemek için teknolojinin kullanımını denetleyecektir.
- Çevrimiçi riskleri belirleme, değerlendirme ve azaltmayöntemleri okulliderliği ekibi tarafından düzenli olarak incelenecektir.

4.2 Daha geniş çapta okul/toplum ortamında internet kullanımı:

- Okul, çevrimiçigüvenlik konusunda ortakbir yaklaşım oluşturmak içinyerel kuruluşlarla irtibat kuracak.

- Okul, internet kullanımının uygun olmasını sağlamak için yerel topluluğun ihtiyaçları (kültürelgeçmişleri, dilleri, dinleri ve etnikkökenleritanımayı da içeren) ile çalışacaktır.
- Okul, okulbilgisayarsistemineveyasitedekiinterneteerişmesigerekenherhangibirkonuk / ziyaretçi için Kabul Edilebilir Kullanım Politikası sağlayacaktır.

4.3 İnternet erişiminin yetkilendirilmesi:

- Okul, okuluncihaz 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 sağlanacakları bildirilecektir.
- Ebeveynlerden, öğrencilerin erişebilmesi için Kabul Edilebilir Kullanım Politikasını okumaları veuygun olduğunda, çocuklarıyla tartışmaları istenecektir.
- Toplumun savunmasız üyeleri için(özel eğitim gereksinimi olan çocuklar gibi)erişimi düşünürken, okul öğrencilerin belirli ihtiyaçları ve anlayışları temelinde kararlaralacaktır.

5. KatılımYaklaşımları:

5.1 Çocukların ve gençlerin katılımı ve eğitimi:

- Öğrenciler arasındagüvenli ve sorumluinternetkullanımınınönemi ile ilgilifarkındalık yaratmak için bir çevrimiçi güvenlik(e-Güvenlik) müfredatı oluşturulur ve okulun tamamında yeralır.
- Güvenli ve sorumlu kullanım ile ilgili eğitim internet erişiminden önce yapılacaktır.
- Müfredat geliştirme ve uygulama da dâhil olmak üzere okul çevrimiçi güvenlik politikaları ve uygulamaları yazarken ve geliştirirken öğrenci katkıları aranacaktır.
- Öğrenciler, Kabul Edilebilir Kullanım Politikasını, yaşlarına ve yeteneklerine uygun bir şekilde okumak ve anlamak için desteklenecektir.
- Tüm kullanıcılara ağve internet kullanımının izleneceği bildirilecektir.
- Çevrimiçi güvenlik (e-Güvenlik) PSHE, SRE, Citizenshipand Computing / BİT programlarına dâhil edilecek ve hem güvenli okul hem de evde kullanımını kapsayacaktır.

  Kabul Edilebilir Kullanım beklentileri ve Posterler, Internet erişimi olan tüm odalarda yayınlanacaktır.
- İnternetin ve teknolojinin güvenli ve sorumlu kullanımı, müfredatta ve tüm konularda güçlenecektir.
- Dışarıdan destek, okulların dâhili çevrimiçi güvenlik(e-Güvenlik) eğitim yaklaşımlarını tamamlamak ve desteklemek için kullanılacaktır.
- Okul, öğrencilerin teknolojiyi olumlu şekilde kullandıklarını ödüllendirecektir.
- Okul, öğrencilerinihtiyaçlarınauygunolarakçevrimiçigüvenliğigeliştirmek içinakran eğitimini uygulayacaktır.

5.2 Savunmasız kabul edilençocukların vegençlerin katılımı ve eğitimi:

Çağlayan Şehit İsmail Dinç Ortaokulu, bir takım faktörlerden dolayı bazı çocukların çevrimiçi ortamda dahasavunmasız olduğunu düşünmektedir.

5.3 Personelin katılımı ve eğitimi:

- Çevrimiçi güvenlik(e-Güvenlik) politikası, tüm çalışanların katılımı için resmi olarak sağlanacak ve tartışılacak ve korunma sorumluluğumuzun bir parçası olarak güçlendirilecek ve vurgulanacaktır.
- Personel,İnternettrafiğininizlenebileceğinivetekbirkullanıcıyakadarizlenebileceğinin farkındaolacak. Okulsistemlerini ve cihazlarını kullanırken takdir yetkisi ve profesyonel davranış gereklidir.
- Personelin tüm üyelerine, profesyonel ve kişisel olarak, güvenli ve sorumlu İnternet kullanımı konusunda güncel ve uygun personel eğitimi, düzenli (en az yıllık) temeldeçeşitli şekillerde sağlanacaktır.
- Çalışanların tüm üyeleri, çevrimiçi davranışlarının okuldaki rolü ve itibarını etkileyebileceğinin farkına varacaktır. Mesleği veya kurumu çürüme durumuna düşürdüğü veya profesyonel yeteneklerine güvenini kaybetmiş bir şeyin bulunduğu düşünülürse, kamusal, disiplin veya hukuki önlemler alınabilir.
- Filtreleme sistemlerini yönetme veya BİT kullanımını izleme sorumluluğu taşıyan personelin üyeleri, Liderlik Ekibi tarafından denetlenecek ve sorunları veya endişeleri bildirmek için açık prosedürlere sahip olacaklar.
- Okul,çalışanlarınöğrencilerinyaşlarınaveyeteneklerinegörekullanmasıgerekenyararlı çevrimiçi araçları vurgulamaktadır.

5.4 Ebeveynlerin katılımı ve eğitimi:

- Çağlayan Şehit İsmail Dinç Ortaokulu, çocukların internetin ve dijital teknolojinin güvenilir ve sorumlu kullanıcıları olabilmesi için ana-babaların oynayacakları önemli bir rolesahip olduklarını kabul eder.
- Ebeveynlerindikkatleri, okulaçıklamaları ve okulwebsitesindeokulçevrimiçigüvenlik(e-Güvenlik) politikasına ve beklentilerine yönelecektir.
- Okul Anlaşması'nınbirparçasıolarakebeveynlerinçevrimiçigüvenlikbilgileriniokumaları istenecektir.
- Ebeveynler, Okula Kabul Edilebilir Kullanım Politikası'nı okumaya ve çocuklarıyla etkilerini tartışmaya teşvik edilecektir.
- Çevrimiçi güvenlik konusundaki ebeveynler için bilgi ve rehberlik, ebeveynlere çeşitli biçimlerde sunulacaktır.
- Ebeveynlerin, çevrimiçi olarak çocukları için olumlu davranışları rol modellemeleri teşvik edilecektir

Çevrimiçi Olaylara ve Koruma sorunlarına yanıt verme:

- Okulun tüm üyeleri, cinsel içerikli mesajlaşma, çevrimiçi / siber zorbalık vb. dâhil olmak üzere karşılaşılabilecek çevrimiçi risklerin çeşitliliğinden haberdar edilecektir. Bu, Öğrencilere yönelik personel eğitimi ve eğitim yaklaşımları içerisinde vurgulanacaktır.
- Okulun tüm üyeleri, filtreleme, cinsel içerikli mesajlaşma, siber zorbalık, yasadışı içerik ihlali vb. gibi çevrimiçi güvenlik (e-Güvenlik) endişelerini bildirme prosedürü hakkında bilgilendirilecektir.
- Dijital Abone Hattı(DSL), daha sonra kaydedilecek olan çocuk koruma endişelerini içeren herhangi bir çevrimiçi güvenlik(e-Güvenlik) olayı hakkında

bilgilendirilecektir.

- İnternet'in yanlışkullanımı ile ilgili şikâyetler, okulunşikâyetprosedürleri kapsamında ele alınacaktır.
- Çevrimiçi/ siberzorbalıkileilgilişikâyetler, okulunzorbalıkkarşıtıpolitikası ve prosedürü kapsamında ele alınacak
- Personelin yanlış kullanımı ile ilgili herhangi bir şikâyet okul müdürüne yönlendirilecektir
- Okul şikâyet prosedürü öğrencilere, velilere ve personele bildirilecektir.
- Şikâyet ve ihbar prosedürü personele bildirilecektir.
- Okulun tüm üyeleri, gizliliğin öneminden ve endişeleri bildirmek için resmi okul usullerine uyma ihtiyacından haberdar olmalıdırlar.
- Okulun tüm üyeleri, çevrimiçi ortamda güvenli ve uygun davranış hakkında hatırlatılacak ve okul camiasının herhangi birdiğerüyesine zararvermek, sıkıntı yaşamak veya suç oluşturan herhangi bir içerik, yorum, resim veya video yayımlamamanın önemini hatırlatacaktır.
- Okul,çevrimiçigüvenlik(e-Güvenlik) olaylarını,uygunolduğunda, okuldisiplini/davranış politikasına uygun olarak yönetir.
- Okul, ebeveynlere, ihtiyaç duyulduğunda bunlarla ilgili endişeleri bildirir.
- Herhangibirsoruşturmatamamlandıktansonraokulbilgialacak, öğrenilendersleri belirleyecek ve değişiklikleri gerektiği gibi uygulayacaktır.
- Sorunlarıçözmek için ebeveynlerinve çocuklarınokulla ortak çalışması gerekir.

Atakan ÖZTEMİR	Hasan DURNA	Barış BOZKURT
Okul Müdürü	Müdür Yardımcısı	Rehber Öğretmen