KOÇARLI ANADOLU LİSESİ MÜDÜRLÜĞÜ STRATEJİK PLANI (2019-2023)

e-Güvenlik (e-Safety) POLİTİKASI

Günlük hayatımızın bir parçası olarak hepimiz dijital teknolojilerle yaşıyoruz. Öğrencilerimizin dijital teknolojiler aracılığıyla mevcut olan fırsatları en iyi nasıl değerlendirebilmelerini sağlamak için, bu teknolojilerinasıl kullanacaklarını bilmek ve anlamak gerekiyor. Bunun en güvenli şekilde ve en güvenli ortamda yapılmasını sağlamak için, öğrencilerimizin evde, okulda, okul dışı ortamlarda, arkadaşlarıyla ya da yalnızolduğu zaman, dikkatini çeken açık ve özlü bir "Güvenli İnternet Okul Politika"sına sahip bir okuluz.

ÖZET

1. Okulumuzun internet sitesi, twitter, vb. gibi sosyal ağları bulunmaktadır. Bu ağların üzerinde yayınlananveriler kontrollü olarak paylaşılmaktadır.
2. Okulumuzda cep telefonları ders esnasında kapalı konumda tutulmakta, eTwinning projesi yapanarkadaşlar proje çalışmaları amacıyla gerektiği takdirde kullanmaktadırlar.
3. Rehberlik servisi tarafından, sınıflara düzenli olarak, BİT bağımlılığı, BİT'nin doğru ve güvenli kullanımı,Siber Zorbalık gibi konularda seminerler tertiplenmektedir.
4. Okulumuzda BİT doğru ve güvenli kullanımı ile ilgili sabit panolar bulunmaktadır.
5. Okulumuzun bazı öğretmenleri Milli Eğitim Bakanlığı tarafından verilen Siber Zorbalık, BİT 'in doğru vegüvenli kullanımı konularında uzaktan ve yüz yüze eğitimler almıştır.
6. Okulumuzda "Daha Güvenli İnternet Günü" kutlanmaktadır (11 Şubat).
7. Okulumuzun internet sitesinde e-güvenlik konusunda, güvenliweb.org.tr. sitesi linki yer almaktadır. Okulpaydaşlarımız istedikleri zaman konu ile ilgili bilgilere ulaşabilmektedirler.
8. Okulumuzda güvenli internet günü kutlamalarında, konu ile ilgili seminerlerde güvenliweb.org.tr.sitesinden alıntılanan bilgi broşürleri dağıtılmaktadır.
9. Rehber Öğretmenlerimiz internet etiği ve güvenli internet kullanımı konuları hakkında öğrencilerimizebilgilerini aktarmaktadır.
10. Okulumuzda 21.yy iletişim becerileri önemsenmektedir. Bununla ilgili olarak öğrencilerimizin BİTkullanım becerilerini geliştirme çalışılmaları yapılmaktadır.
11. Okulumuzda Dijital vatandaş olma konusunda paydaşlarımızı bilinçlendirme çalışmaları yapılmaktadır.

e-GÜVENLİK POLİTİKASININ AMACI

- Koçarlı Anadolu Lisesi'nin tüm üyelerini çevrimiçi olarak korumak ve güvenliğini sağlamak.
- Teknolojinin potansiyel riskleri ve yararları konusunda idareci, öğretmeni öğrenci ve çalışanları için 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 politikanın, yönetim organı, öğretmenler, destek personeli, harici yükleniciler, ziyaretçiler, gönüllüler ve okul adına hizmet veren veya bunları yerine getiren diğer kişiler (toplu olarak bu politikada 'personel' olarak anılacaktır.) dahil olmak üzere tüm personel için geçerlidir) yanı sıra çocuklar ve ebeveynleri kapsamasını sağlamak.

Sonuç olarak ana hedefimiz, internet erişimi ve kişisel cihazlar da dahil olmak üzere bilgi iletişim cihazlarının kullanımı için bu güvenlik politikasının geçerli olmasıdır. Dizüstü bilgisayarlar, tabletler veya mobil cihazlar gibi uzaktan kullanım için okul tarafından verilen cihazlar için de geçerlidir.

Tüm Çalışanların Kilit Sorumlulukları

- Çevrimiçi güvenlik politikalarının geliştirilmesine katkıda bulunmak.
- Kabul Edilebilir Kullanım Politikalarını (AUP'lar) okumak ve onlara bağlı kalmak.
- Okul sistemlerinin ve verilerin güvenliğinden sorumlu olmak.
- Bir dizi farklı çevrimiçi güvenlik konusundaki farkındalığa sahip olmak ve onların bakımında çocuklarla nasıl ilişkili olabileceklerini bilmek.
- Yeni ve gelişmekte olan teknolojiler kullanıldığında iyi uygulamaları modelleme
- Mümkün olduğunca müfredat ile çevrimiçi güvenlik eğitimini ilişkilendirme.
- Okul koruma politikalarını ve prosedürlerini takip ederek endişe duyan bireylerin belirlenmesi ve uygun önlem alınması.
- Olumlu öğrenme fırsatlarına vurgu yapmak.
- Bu alanda mesleki gelişim için kişisel sorumluluk almak.

Çocukların ve Gençlerin Başlıca Sorumlulukları

- Çevrimiçi güvenlik politikalarının geliştirilmesine katkıda bulunmak.
- Okulun Kabul Edilebilir Kullanım Politikalarını okumak ve onlara bağlı kalmak.
- Çevrim içi ve çevrimdışı başkalarının hislerine ve haklarına saygı duymak.
- İşler ters giderse, güvenilir bir yetişkinden yardım istemek ve çevrimiçi güvenlik sorunlarıyla karşılaşan diğer kişileri desteklemek.

<u>Yaşlarına, yeteneklerine ve zayıf yönlerine uygun bir seviyede:</u>

- Kendilerini ve başkalarını çevrimiçi olarak korumak için sorumluluk almak.
- Yeni ve gelişmekte olan teknolojilerin getirdiği fırsatlar ve risklerle ilgili olarak kendi bilinci ve öğrenimlerinden sorumlu olmak.

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

Ebeveynlerin Başlıca Sorumlulukları

- Okul Kabul Edilebilir Kullanım Politikalarını okumak, çocuklarını bu politikaya bağlı kalmaya teşvik etmek ve uygun olduğunca kendilerinin de bağlı kalmasını sağlamak.
- Çocuklarıyla çevrimiçi güvenlik konularını tartışmak, okulun çevrimiçi güvenlik yaklaşımlarını desteklemek ve evde uygun güvenli çevrimiçi davranışları pekiştirmek.
- Teknoloji ve sosyal medyanın güvenli ve uygun kullanımını modellemek.
- Davranışlarında, çocuğun çevrimiçi olarak zarar görme tehlikesi altında olduğunu gösteren değişiklikleri belirlemek.
- Okul veya diğer uygun kurumlardan, kendileri ve ya çocukları çevrimiçi problem veya sorunlarla karşılaşırsa yardım veya destek istemek.
- Okulun çevrimiçi güvenlik politikalarının oluşturulmasına katkıda bulunmak.
- Öğrenme platformları ve diğer ağ kaynakları gibi okul sistemlerini güvenli ve uygun bir şekilde kullanmak.
- Yeni ve gelişmekte olan teknolojilerin getirdiği fırsatlar ve risklerle ilgili olarak kendi bilinci ve öğrenimlerinden sorumlu olmak.

OKULUN ÇEVİRİM İÇİ VARLIĞI

- Web sitesinde iletişim bilgileri okul adresi, e-posta ve telefon numarası olacaktır. Personel veya öğrencilerin kişisel bilgileri yayınlanmayacaktır.
- Okul Müdürü yayınlanan çevrimiçi içerik için genel yayın sorumluluğunu alacak ve bilgilerin doğru ve uygun olmasını sağlayacaktır.
- Web sitesi, erişilebilirlik fikri mülkiyet haklarına saygı, gizlilik politikaları ve telif hakkı da dahil olmak üzere okulun yayın yönergelerine uyacaktır.
- Spam maillerden korunmak için e-posta adresleri çevrimiçi olarak dikkatli bir şekilde yayınlanacaktır.
- Öğrenci çalışmaları öğrencilerin izniyle ya da ebeveynlerinin izniyle yayınlanacaktır.
- Okul web sitesinin yönetici hesabı, uygun bir şekilde güçlü şifreyle şifrelenerek korunacaktır.
- Okul, çevrimiçi güvenlik dahil olmak üzere, toplumun üyeleri için okul web sitesinde korunma hakkında bilgi gönderecektir.
- 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.

ÇEVRİMİÇİ İLETİŞİM VE TEKNOLOJİNİN GÜVENLİ KULLANIMI

Öğrenci ve Personelin Teknolojiye Erişimi

Okul binalarımızda bilgi teknolojileri açısından son derece önemli olan network alt yapısı bu alanda en gelişmiş ürünler ile gerçekleştirilmiştir. Kampus network alt yapısı, binalar arasında yer altında bulunan tünellerden ana merkeze bağlı fiber optik kablolama ile yapılmıştır.

Okulumuz 2020 yılında wifi alt yapısı ile desteklenmiş olup mevcut hız arttırılmıştır. Öğrencilerimiz ve öğretmenlerimiz, internet erişimi ve çalışma ortamı sağlanması amacıyla bilgisayarlardan, akıllı tahtalardan, tablet ve telefonlarından yararlanmaktadırlar. Okul bilgisayarların hepsi okul network ağında çalışmaktadır.

Okulumuz bilgisayarlarında kullanılan filtre programı ile zararlı sitelere giriş önlenmektedir. Böylece öğrencilerimizin interneti sadece eğitim amaçlı kullanmaları sağlanmaktadır.

Okul / Web Sitesinin Yönetilmesi

- Web sitesinde iletişim bilgileri okul adresi, e-posta ve telefon numarası olacaktır. Personel veya öğrencilerin kişisel bilgileri yayınlanmayacaktır.
- Okul Müdürü yayınlanan çevrimiçi içerik için genel yayın sorumluluğunu alacak ve bilgilerin doğru ve uygun olmasını sağlayacaktır.
- Web sitesi, erişilebilirlik fikri mülkiyet haklarına saygı, gizlilik politikaları ve telif hakkı da dahil olmak üzere okulun yayın yönergelerine uyacaktır.
- Spam maillerden korunmak için e-posta adresleri çevrimiçi olarak dikkatli bir şekilde yayınlanacaktır.
- Öğrenci çalışmaları öğrencilerin izniyle ya da ebeveynlerinin izniyle yayınlanacaktır.
- Okul web sitesinin yönetici hesabı, uygun bir şekilde güçlü şifreyle şifrelenerek korunacaktır.
- Okul, çevrimiçi güvenlik dahil olmak üzere, toplumun üyeleri için okul web sitesinde korunma hakkında bilgi gönderecektir.

Çevrimiçi Görüntü ve Videolar Yayınlama

- Okul, çevrimiçi paylaşılan tüm resimlerin ve videoların okul resim kullanımı politikasına uygun şekilde kullanılmasını sağlayacaktır.
- Okul , resimlerin ve videoların tümünün, veri güvenliği, Kabul Edilebilir Kullanım Politikaları, Davranış Kuralları, sosyal medya, kişisel cihazların ve cep telefonlarının kullanımı gibi diğer politikalar ve prosedürlere uygun şekilde yer almasını sağlayacaktır.

- Görüntü politikasına uygun olarak, öğrencilerin resimlerinin / videolarının elektronik olarak yayınlanmasından önce her zaman ebeveynlerin yazılı izni alınacaktır.

Video Konferans Kuralları

- Öğrenciler, bir video konferans araması veya mesajı hazırlamadan veya cevaplamadan önce bir öğretmenin izin isteyecektir.
- Video konferans, öğrencilerin yaşı ve yeteneği için uygun bir şekilde denetlenecek.
- Velilerin rızası, çocuklar video konferans faaliyetlerine katılmadan önce alınacaktır.
- Video konferans, sağlam bir risk değerlendirmesini takiben, resmi ve onaylanmış iletişim kanalları vasıtasıyla gerçekleşecektir

- Sadece ana yöneticilere video konferans yönetim alanlarına veya uzaktan kumanda sayfalarına erişim hakkı verilecektir.
- Eğitimsel video konferans servisleri için özel oturum açma ve şifre bilgileri yalnızca personellere verilecek ve gizli tutulacak.

Kişisel Cihazların ve Cep Telefonlarının Kullanımı

- Cep telefonlarının ve çocukların, gençlerin ve yetişkinler arasındaki diğer kişisel cihazların yaygın bir şekilde sahiplenilmesi, tüm üyelerin 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 tarafından kararlaştırılacak ve okul Kabul Edilebilir Kullanım veya Cep Telefonu Politikası dahil olmak üzere uygun politikalarda yer alacaktır.
- Koçarlı Anadolu Lisesi, mobil teknolojilerle yapılan kişisel iletişimin, çocuklar, personel ve anne-babalar için gündelik yaşamın kabul edilen bir parçası olduğunun farkındadır; ancak bu tür teknolojilerin okulda güvenli ve uygun bir şekilde kullanılmasını gerektirir.

Öğrencilerin Kişisel Cihazlarını ve Cep Telefonlarını Kullanımı

- Öğrenciler, kişisel cihazların ve cep telefonlarının güvenli ve uygun kullanımı konusunda eğitim alacaklardır.
- Bilişim araçlarını, okul yönetimi ile öğretmenin bilgisi ve izni dışında konuşma yaparak, ses ve görüntü alarak, mesaj ve e-mail göndererek, bunları arkadaşlarıyla paylaşarak eğitim-öğretimi olumsuz yönde etkileyecek şekilde kullanmak aynı zamanda okul ders saatleri içerisinde telefon bulundurmak kesinlikle yasaktır.
- Öğrenciler ders başlamadan önce telefonlarını okul yönetimi tarafından yaptırılan telefon kutularına koymakla yükümlüdür. Cep telefonunun amacı dışında kullanımı ihlali oluştuğunda, öğrenci, telefondaki özel verilerin korunmasını sağlamak amacıyla telefonunu kapatıp ders öğretmenine verir. Ders öğretmeni öğrenci telefonunu ilgili müdür yardımcısına teslim eder. Cep telefonu öğrenci velisine teslim edilinceye kadar güvenli bir yerde tutulur. Velisi dışında telefon kimseye teslim edilmez.
- Çocukların cep telefonlarının ve kişisel cihazların tüm kullanımları, kabul edilebilir kullanım politikasına uygun olarak gerçekleşecektir.
- Cep telefonları veya kişisel cihazlar, bir öğretmenin onayını alarak onaylanmış ve yönlendirilmiş müfredat tabanlı etkinlik kapsamında olmadıkları sürece dersler veya resmi okul saatlerinde öğrenciler tarafından kullanılamaz.
- Çocukların cep telefonlarını veya kişisel cihazlarını eğitim etkinliğinde kullanımı, okul idaresi tarafından onaylandığında gerçekleşecektir.

- Bir öğrenci ebeveynlerini arama gereği duyduğunda, okul telefonunu kullanmasına izin verilecektir.
- Ebeveynlerin okul saatlerinde cep telefonuyla çocuklarıyla iletişim kurmamaları, okul idaresine başvurmaları önerilir. İstisnai durumlarda öğretmenin onayladığı şekilde istisnalara izin verilebilir.
- Öğrenciler, telefon numaralarını yalnızca güvenilir arkadaşlarına ve aile üyelerine vermelidirler.
- Öğrencilere, cep telefonlarının ve kişisel cihazların güvenli ve uygun bir şekilde kullanımı öğretilecek ve sınırların ve sonuçların farkına varılacaktır.
- Öğrencinin kişisel cihazında veya cep telefonunda bulunan materyalin yasadışı olabileceği veya cezai bir suçla ilgili kanıt sağlayabileceğinden şüpheleniliyorsa, cihaz daha ayrıntılı araştırma için polise teslim edilir.

Ziyaretçiler Kişisel Cihazların ve Cep Telefonlarının Kullanılması

- Ebeveynler ve ziyaretçiler, okulun kabul edilebilir kullanım politikasına uygun olarak cep telefonlarını ve kişisel cihazları kullanmalıdır.
- Fotoğraflar veya videolar çekmek için ziyaretçiler ve ebeveynler tarafından cep telefonlarının veya kişisel cihazların kullanılması, okul resim kullanımı politikasına uygun olarak gerçekleştirilmelidir.
- Okul, ziyaretçilere kullanım beklentilerini bildirmek için uygun tabela ve bilgileri sağlayacak ve sunacaktır.
- Personelin uygun ve güvenli olduğunda sorunlara karşı çıkması beklenir ve her zaman ziyaretçilerin herhangi bir ihlalini idareye bildirecektir.

Çocukların, Gençlerin Katılımı ve Eğitimi

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

Personelin Katılımı ve Eğitimi

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

- Personel, İnternet trafiğinin izlenebileceğini ve tek bir kullanıcıya kadar izlenebileceğinin farkında olacak. Okul sistemlerini ve cihazlarını kullanırken takdir yetkisi ve profesyonel davranış gereklidir.
- Personelin tüm üyelerine, profesyonel ve kişisel olarak, güvenli ve sorumlu İnternet kullanımı konusunda güncel ve uygun personel eğitimi, düzenli (en az yıllık) temelde çeşitli şekillerde sağlanacaktır.
- Çalışanların tüm üyeleri, çevrimiçi davranışlarının okuldaki rolü ve itibarını etkileyebileceğinin farkına varacaktır. Mesleği veya kurumu çürüme durumuna düşürdüğü veya profesyonel yeteneklerine güvenini kaybetmiş bir şeyin bulunduğu düşünülürse, kamusal, disiplin veya hukuki önlemler alınabilir.
- Filtreleme sistemlerini yönetme veya BİT kullanımını izleme sorumluluğu taşıyan personelin

üyeleri, Liderlik Ekibi tarafından denetlenecek ve sorunları veya endişeleri bildirmek için açık prosedürlere sahip olacaklar.
- Okul, çalışanların öğrencilerin yaşlarına ve yeteneklerine göre kullanması gereken yararlı çevrimiçi araçları vurgulamaktadır.

Ebeveynlerin Katılımı ve Eğitimi

- Koçarlı Anadolu Lisesi, çocukların internetin ve dijital teknolojinin güvenilir ve sorumlu kullanıcıları olabilmesi için ana-babaların oynayacakları önemli bir role sahip olduklarını kabul eder.
- Ebeveynlerin dikkatleri, okul açıklamaları ve okul web sitesinde okul çevrimiçi güvenlik (e-Güvenlik) politikasına ve beklentilerine yönelecektir.
- Okulumuzun bir parçası olarak ebeveynlerin çevrimiçi güvenlik bilgilerini okumaları 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, sakıncalı mesajlaşma, çevrimiçi / siber zorbalık vb. dahil olmak üzere karşılaşılabilecek çevrimiçi risklerin çeşitliliğinden haberdar edilecektir. Bu, öğrencilere yönelik personel eğitimi ve eğitim yaklaşımları içerisinde vurgulanacaktır.
- Okulun tüm üyeleri, filtreleme, sakıncalı mesajlaşma, siber zorbalık, yasadışı içerik ihlali vb. gibi çevrimiçi güvenlik (e-Güvenlik) endişelerini bildirme prosedürü hakkında bilgilendirilecektir.
- Dijital Abone Hattı (DSL), daha sonra kaydedilecek olan çocuk koruma endişelerini içeren herhangi bir çevrimiçi güvenlik (e-Güvenlik) olayı hakkında bilgilendirilecektir.
- İnternet'in yanlış kullanımı ile ilgili 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 okul müdürüne yönlendirilecektir
- Okul şikayet prosedürü öğrencilere, velilere ve personele bildirilecektir.
- Şikayet ve ihbar prosedürü personele bildirilecektir.
- Okulun tüm üyeleri, gizliliğin öneminden ve endişeleri bildirmek için resmi okul usullerine uyma ihtiyacından haberdar olmalıd

- Okulun tüm üyeleri, çevrimiçi ortamda güvenli ve uygun davranış hakkında hatırlatılacak ve okul camiasının herhangi bir diğer üyesine zarar vermek, sıkıntı yaşamak veya suç oluşturan herhangi bir içerik, yorum, resim veya video yayımlamamanın önemini hatırlatacaktır.
- Okul, çevrimiçi güvenlik (e-Güvenlik) olaylarını, uygun olduğunda, okul disiplini / davranış politikasına uygun olarak yönetir.
- Okul, ebeveynlere, ihtiyaç duyulduğunda bunlarla ilgili endişeleri bildirir.
- Herhangi bir soruşturma tamamlandıktan sonra okul bilgi alacak, öğrenilen dersleri belirleyecek ve değişiklikleri gerektiği gibi uygulayacaktır.
- Sorunları çözmek için ebeveynlerin ve çocukların okulla ortak çalışması gerekir.

RESİM KULLANIMI POLİTİKASI

- Okul idaresi tarafından görevli kılınanlar haricindeki kişiler tarafından ve öğrenci velilerinin bilmek istedikleri etkinlik ve programlar dışındaki zamanlarda , okul ve okul bahçesi sınırları içerisinde fotoğraf ve video çekimi yapılamaz. Bu yasak bir öğrencinin diğer bir öğrencinin fotoğraf ve videosunu çekmek istemesi durumunda da geçerlidir.
- Okul idaresi tarafından görevlendirilen kişilerin çektiği fotoğraf ve videolar ancak Okulun resmi web adresinde ve sanal ortamlarında, ilgili öğrenci velisinin talep ve yazılı onayı ile yayınlanabilir. Öğrencisi için onay vermeyen velinin öğrencisi ile ilgili fotoğraf ve videolar yayınlanmaz.
- Velisi tarafından fotoğraf ve video görüntülerinin çekilip yayınlanmasına onay verilmeyen öğrencilerin, çekim esnasında psikolojik baskı yaşamaması için tedbirler alınır.
- Okul görevlileri tarafından yayınlanan resim ve videolarda öğrencilerin kişisel bilgilerine kesinlikle yer verilmez. Öğrenciler, bir video konferans araması veya mesajı hazırlamadan veya cevaplamadan önce bir öğretmenin izin isteyecektir. Video konferans, öğrencilerin yaşı ve yeteneği için uygun bir şekilde denetlenecek. (okullar bunun nasıl uygulanacağını ve başarılacağını listelemelidir) Veliler ve bakıcıların rızası, çocuklar video konferans faaliyetlerine katılmadan önce edinilecektir. 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 verilmektedir. Eğitimli video konferans servisleri için benzersiz oturum açma ve şifre bilgileri yalnızca personel üyelerine verilecek ve güvence altına alınmış olacak.

- **GENEL VERİ KORUMA VE SINIFLANDIRMA POLİTİKASI**

- Kurum içi bilgi paylaşımı sadece görev gereği ilgili veriye ulaşması gereken kullanıcılar arasında olmalıdır. Kurumsal web sitelerinden (www.meb.gov.tr gibi) yapılan yayın da dahil olmak üzere halka aktarılacak bilgiler, aktarılan verinin sınıflandırması da göz önüne alınmak kaydı ile, sadece Kurumsal İletişim bölümü tarafından belirlenir ve bu bölümden sorumlu yöneticinin atayacağı kişiler tarafından bu bilgiler halka ulaştırılır.

Veri Sahipliği ve Sınıflandırılması

- Kullanıcılar kendileriyle ilgili iş verilerinin sahibi olup bu varlıkların korunmasından nihai olarak sorumludur. Veri sahipleri kendileriyle ilgili iş verilerinin sınıflandırılmasından ve gerektiğinden yeniden sınıflandırılmasından sorumludur. Verinin çevrim içi saklanabileceği gibi, çevrim dışı ve basılı doküman halinde de saklanabileceği unutulmamalıdır.

Kurumsal Verinin Saklanması

- Kullanıcılar sahibi oldukları iş verilerinin yasal yükümlülükler veya iş gereklerinden doğan saklanma süre ve şart ihtiyaçlarını BİT Sorumlusu'na bildirmekle yükümlüdür. Basılı dokümanlar üzerinde bulunan veriler de bu maddenin kapsamı içindedir. Genel prensip olarak üzerinde çalışılan dosyalar ve kritik olmayan dosyalar kişisel bilgisayarlarda saklanabilir, ancak kritik dosyalar üzerinde çalışılmadığı durumlarda kişisel bilgisayarlardan silinmeli ve sunucularda saklanmalıdır. Kullanıcılar veri saklama konusunda Koçarlı Anadolu Lisesiveri saklama prosedür ve yöntemlerini kendi yöntemlerine tercih etmeli, sahibi oldukları kritik verilerin kurumsal yedekleme prosedürlerine dahil olduğundan emin olmalıdır.

Diz Üstü Bilgisayarlar, Tablet Bilgisayarlar ve Akıllı Telefonlar

- Diz üstü bilgisayar Koçarlı Anadolu Lisesitarafından satın alınıp, ilgili işletim sistemi, ilgili programlar ve gereken güvenlik uygulamaları BİT Teknik Destek birimi tarafından yüklenir.

- Gerek Koçarlı Anadolu Lisesitarafından verilen akıllı telefonlar, gerekse personele ait kişisel ve iş amaçlı kullanılan akıllı telefonlar merkezi olarak güvenlik yönetimine tabidir. Bu kapsamda SOTI, MERAKI gibi uygulamar ile bu cihazlar uzaktan yönetilmekte ve kontrol edilmektedir. Koçarlı Anadolu Lisesipersoneli; kullandığı telefon cinsine göre (Iphone, BlackBerry,Windows, Android İşletim Sistemli) ve/veya kullandığı tablet bilgisayar cinsine göre (Ipad, Android, Windows İşletim Sistemi) Koçarlı Anadolu Lisesitarafından bu bağlamda belirlenen güvenlik yöntemlerini uygulamak zorundadır.

- Bunun yanında kullanıcılar, hassas kurum verilerini KOÇARLI ANADOLU LİSESİdiz üstü bilgisayarlarında, tablet bilgisayarlarında ve akıllı telefonlarında saklamaktan kaçınmalıdır. Yöneticileri tarafından izin verildiği takdirde personele zimmetlenen tüm mobil cihazlar, varlık sahipleri tarafından Koçarlı Anadolu Lisesisınıfları dışına çıkarılmaya uygundur. Bu cihazlar taşınabilir olmaları ve kurum dışında da bulunabilmeleri dolayısı ile çalınma tehdidine daha duyarlıdır. Bu nedenle bu cihazların kullanıcıları özellikle halka açık mekanlarda cihazlarını terk etmemeli ve fiziksel güvenliğini sağlamalıdır. Taşınabilir cihazlar Koçarlı Anadolu Lisesinauzaktan erişim için kullanılıyorsa erişim için kullanılan kullanıcı adı ve parola bilgileri bilgisayar üzerinde herhangi bir dosya içinde saklanmamalıdır.

Ofisleri Dışına Gönderilen Bilgisayarlar ve Veri Saklama Araçları

- Koçarlı Anadolu Lisesinaait kişisel bilgisayarlar veya bu bilgisayarlara ait depolama birimleri tamir veya hibe amacı ile kurum dışına gönderilecekse, bu bilgisayarların kullanıcıları bilgisayar üzerinde bulunan hassas verilerin silinmesi ve gerekiyorsa yedeklenmesinden nihai olarak sorumludur. Normal yöntemler ile silinen dosyalar tekrar elde edilebildiğinden kullanıcılar güvenli silme konusunda BİT sorumlusuna başvurmalı ve teknik destek talep etmelidir. Ofis dışına gönderilen diğer bilgisayarlar için veri temizleme sorumluluğu Koçarlı Anadolu LisesiTeknik Destek Uzmanları'na aittir. Ofis dışına gönderilen her türlü bilgisayar, veri saklama aracı gibi cihazlar için Bilgisayarlar ve Veri Saklama Araçları Teslim Tutanağı'nın doldurulması zorunludur.

- **Koçarlı Anadolu LisesiAğına Uzaktan Erişim**

- Koçarlı Anadolu Lisesiağına VPN ile uzaktan erişmesi gereken kullanıcılar erişim için, sıra dışı bir neden yoksa, Koçarlı Anadolu Lisesinaait diz üstü bilgisayarlarını

kullanmalıdır. Kullanıcılar uzaktan erişim araçlarını (parola, sertifika, PIN kodu v.b. gibi) koruma

- konusunda diğer erişim araçlarının korunmasına nazaran daha üstün hassasiyet göstermelidir. Uzaktan erişim kimlik doğrulama için kullanılan cihazların üzerine Koçarlı Anadolu Lisesiveya kullanıcıyla ilgili bir erişim bilgisi (telefon numarası, sunucu adı, IP adresi, kullanıcı kodu, v.b. gibi) yazılmamalı / yapıştırılmamalıdır. Eğer sıra dışı bir durum için Koçarlı Anadolu Lisesibilgisayarı dışında bir bilgisayardan uzaktan erişim yapılması gerekiyorsa BİT Destek Sorumlusu'nun onayı alınmalıdır. Halka açık bilgisayarların uzaktan erişim için kullanımı her koşulda yasaktır.

Temiz Masa, Temiz Ekran Politikası

- Kullanıcılar ofis masaları başında olmadıklarında hassas bilgi içeren basılı dokümanları masa üstünde bırakmamalıdır. Hassas bilgi içeren basılı dokümanlar kullanılmadıklarında masadan kaldırılmalı ve gerekiyorsa kilit altında tutulmalıdır.
- Kullanıcılar kurum dışında basılı doküman, bilgisayarlar ve veri saklama cihazlarının fiziksel güvenliği konusunda çok hassas davranmalı, asla kontrolsüz biçimde açıkta bırakmamalıdır. Kurum dışında bilgisayar ekranından veya basılı dokümanlardan hassas bilgilerin başkalarınca izlenme riskinin daha yüksek olduğu unutulmamalı, halka açık mekanlarda hassas bilgiler görüntülenmemelidir. Kullanıcılar her ne sebep ile olursa olsun, Koçarlı Anadolu Lisesisınıfları içinde veya farklı bir alanda, bilgisayarının başından ayrılırken ekranını (Windows ve L tuşlarına aynı anda basarak) kilitlemelidir.

Telefon Görüşmeleri

- Koçarlı Anadolu Lisesiçalışanları özellikle Koçarlı Anadolu Lisesidışında hassas bilgileri içeren telefon görüşmesi yapmamaya gayret etmelidir. Hassas bilgilerin iletişimini gerektiren bir görüşme yapılması gerekiyorsa cep telefonları diğer şahıslara / kurumlara ait telefonlara, kapalı ve yalnız bulunulan mekanlar tercih edilmeli, açık mekanlar tercih edilmemelidir.

BT YÖNETİMİ POLİTİKASI

AMAÇ

- Bu politikanın amacı; Koçarlı Anadolu LisesiBT yazılım yönetim sistemi prensiplerini tanımlamak ve bu prensiplere okul yönetiminin verdiği desteği ifade etmektir.

SORUMLULUK

BT Üst Yönetim

- BT Yönetimi Politikasının okul ihtiyaçlarını karsılar nitelikte bulunmasından ve politikanın uygulanması için gerekli destek ve gözetimin sağlanmasından, politikanın en az yılda bir kez veya okul politikasında değişiklik gerektirebilecek durumlarda gözden geçirilmesinden sorumludur.

Kurum BT Yöneticisi

- BT Yöneticisi,BT Yazılım Yönetim sistemi Politikasının şirket ihtiyaçlarını karşılar nitelikte
- kurgulanmasından, uygulanması için gerekli destek ve gözetimin sağlanmasından sorumludur.

KAPSAM

- Bu politikanın kapsamı tüm organizasyondur.

UYGULAMA

- Bilgi Teknolojileri BT Yazılım Yönetim Sistemi Politikası

- Sürüm Yönetimi Süreci ile kullanılmakta olan tüm yazılımların sürüm vb. dahil izlenmesi ve ilişkili süreçlere bağlı olarak güncellenmesini sağlayarak sınıflarda, öğretmen ve öğrencilerce doğru sürümleri kullanmak. Toplu güncellemeleri yönetmek.

YAPTIRIM

- Bu politikaya uygun olarak çalışmayan tüm personel hakkında 657 Sayılı Devlet Memurları Kanunu Disiplin Yönetmeliği ve Ortaöğretim Kurumları Yönetmeliği prosedürü uygulanır.

E- GÜVENLİK EKİBİ

Levent ARAS

Gülin AYDIN

Tunahan BOZKURT

Mevlüt ERTEN

Okul Müdürü