



Emlakbank Süleyman Demirel Anadolu Lisesi

E-Güvenlik Vizyonu

Okulumuzun e-güvenlik vizyonu, dijital ortamların hızla geliştiği ve yayıldığı bir zaman diliminde dünyaya gelen ve bu dünya ile iç içe büyüyen öğrencilerimizin bu ortamlarda güvenli kalmalarını sağlamak ve ek olarak bilinçli ve bilgili birer medya okur yazarı olarak yetişmelerini amaçlamaktır.

Emlakbank Süleyman Demirel Anadolu Lisesi

E-Güvenlik Politikası

Dünya ve eğitim sistemi tüm dünyada hızla değişiyor ve gelişiyor. Günümüzde teknoloji ve internet kullanımı birçok insanın özellikle de Z kuşağı olarak adlandırılan yeni neslin ayrılmaz bir parçası olmaktadır. Her alanda olduğu gibi eğitimde de teknoloji ve internet kullanımı vazgeçilmez ve hatta zorunlu hale gelmektedir. İnternetin bizlere sağladığı kolaylıklar ve avantajlar yadsınamaz. Fakat bunun yanında, bilinçli ve güvenli kullanılmadığı takdirde bireysel ve toplumsal yıkımları da bir gerçektir. Bu sebeple Emlakbank Süleyman Demirel Anadolu Lisesi olarak dijital güvenlik kavramının önemini anlamakta ve gençlerimizin ve yetişkinlerin riski yönetme ve bunları anlama stratejilerini nasıl geliştireceklerini öğrenebilmeleri, çevrimiçi uygulamaları geliştirmeleri için desteklemektedir.

1) AMAÇ

1. Teknolojinin potansiyel riskleri ve yararları konusunda Emlakbank Süleyman Demirel Anadolu Lisesi idarecileri, öğretmenleri, öğrencileri ve çalışanları için farkındalık yaratmak.
2. 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.
3. Güvenli ve emniyetli bir ortam olmasını sağlamak için güvenli ve sorumlu kullanım teknolojisi konusunda okulumuzun tüm üyelerinden beklenen temel ilkeleri açıkça belirtmek.
4. Okulumuzun tüm üyelerini çevrimiçi olarak korumak ve güvenliğini sağlamak.
5. Toplumun eğitim standartlarını yükseltmek, eğitim ve öğrenim deneyiminin bir parçası olarak çevrim içi teknolojiye güvenli erişim için güvenli ve zenginleştirici bir ortam sağlamak, personelin profesyonel çalışmalarını desteklemek ve yönetim işlevlerini geliştirmek için kaliteli İnternet erişimi sağlamak.

2) KAPSAM

Bu politika, okul yöneticileri, öğretmenler, öğrenciler, veliler, destek personeli, ziyaretçiler, gönüllüler ve okul adına hizmet veren veya bunları yerine getiren diğer kişiler de dahil olmak üzere tüm personel için geçerlidir.

3) E-GÜVENLİK (E-SAFETY) POLİTİKAMIZ

1. Okulumuzda ders anlatımı yapılan her alanda etkileşimli tahta ve güvenli internet erişim ağı vardır. Ders anlatımlarında EBA Eğitim ve e-Twinning portallarından da yararlanılmaktadır. Güvenli internet erişim ağı, ağ güvenlik filtresiyle kullanılmaktadır.

2. Okulumuzun internet sitesi ve instagram sosyal ağında hesabı bulunmaktadır. Bu ağların üzerinde yayınlanan veriler kontrollü olarak paylaşılmaktadır.
3. Etkileşimli tahtalar güvenlik kurulumu ile öğretmenlerin kontrolünde kullanılmaktadır.
4. Okulumuzda öğrencilerin cep telefonları, ders saatleri içerisinde okul idaresi tarafından sınıflarda yaptırılan telefonlar için yapılmış olan özel bölüme konulmaktadır.
5. Rehberlik servisi ve Bilişim Teknolojileri öğretmeni tarafından, tüm sınıf seviyelerinde düzenli olarak, BİT bağımlılığı, BİT'nin doğru ve güvenli kullanımı, Siber Zorbalık gibi konularda seminerler tertiplenmektedir.
6. Okulumuzda BİT doğru ve güvenli kullanımı ile ilgili sabit pano bulunmaktadır.
7. Okulumuzda etkileşimli tahtalar, güvenli erişim ağı ve EBA Eğitim ve e-Twinning portallarının kullanımının olması nedeniyle zümre öğretmenleri tarafından her zümrede BİT'nin doğru ve güvenli kullanımı, yapılan alıntıların derslere ve ödevlere aktarımı(kaynak kullanımı) ile ilgili kararlar alınmakta ve öğrenciler bu yönde bilgilendirilmektedir.
8. Okulumuzun öğretmenleri Milli Eğitim Bakanlığı tarafından verilen Siber Zorbalık, BİT'in doğru ve güvenli kullanımı konularında uzaktan ve yüz yüze eğitimler almıştır/alacaktır.
9. Okulumuzda "Güvenli İnternet Günü" kutlanmaktadır.
10. Okulumuzun internet sitesinde e-güvenlik konusunda, guvenliweb.org.tr. sitesi ve buradan alıntılanan öğrenci ve velilere yönelik videolar ve afişler yer alan linkler yer almaktadır.
11. Okul paydaşlarımız istedikleri zaman konu ile ilgili bilgi alabilmekteler.
12. Okulumuzda güvenli internet günü kutlamalarında, konu ile ilgili seminerlerde guvenliweb.org.tr. sitesinden alıntılanan bilgi broşürleri dağıtılmaktadır.
13. Ders içeriklerine internet etiği ve güvenli internet kullanımı konuları eklenerek öğrencilerimize aktarılmaktadır.
14. Okulumuzda 21.yy iletişim becerileri önemsenmektedir. Bununla ilgili olarak öğrencilerimizin BİT kullanım becerilerini geliştirme çalışmaları yapılmaktadır.
15. Okulumuzda Dijital vatandaş olma konusunda paydaşlarımızı bilinçlendirme çalışmaları yapılmaktadır.
16. Okulumuzda izinsiz fotoğraf çekmek kesinlikle yasaktır.
17. Okulumuzun öğrencilerinin yüzleri okula ait sosyal medya sitesinde ve eTwinning portalı dahilindeki proje resimlerinde gösterilmeden önce velilerinden mutlaka Açık Rıza Beyan Formu alınmaktadır/alınacaktır.
18. Öğrencilerimizin ve velilerimizin okulumuza kayıt olurken sağladıkları kişisel bilgileri idare sorumluluğunda ve tarafından korunmaktadır.
19. Velilerimizin iletişim bilgileri kendi bilgi ve istekleri haricinde asla 3. Şahıslarla paylaşılamaz.

4) SORUMLULUKLAR

Yönetim Organı ve Liderlik Ekibinin Temel Sorumlulukları:

1. Okul topluluğu genelinde uygun destek ve danışma ile ulusal ve yerel öneriler doğrultusunda çevrimiçi güvenlik vizyonunu ve kültürünü tüm paydaşlarla geliştirmek ve teşvik etmek .
2. Çevrimiçi güvenliğin tüm topluluk tarafından bir koruma sorunu olarak görülmesini sağlamak ve sağlam bir çevrimiçi güvenlik kültürü geliştirmek.
3. Çevrimiçi güvenlik rollerini ve sorumluluklarını yerine getirmek için yeterli zaman ve kaynağa sahip olmalarını sağlayarak Belirlenen Koruma Liderini (DSL) desteklemek.
4. Uygun profesyonel davranış ve teknoloji kullanımını kapsayan Kabul Edilebilir Kullanım Politikası (AUP) dahil olmak üzere çevrimiçi güvenliğe ilişkin uygun ve güncel politika ve prosedürleri sağlamak.
5. Öğrencileri, okul eğitiminin gereksinimlerini karşılayan uygunsuz içerikten korumak ve aynı zamanda öğrencilerin gerekli eğitim materyallerine erişimini sağlamak için uygun filtreleme ve izleme sistemlerinin mevcut olmasını sağlamak.
6. Okul / ayar sistemleri ve ağlarının emniyet ve güvenliğinin izlenmesinde teknik personel ile çalışmak ve bunları desteklemek ve okul / ayar ağ sisteminin aktif olarak izlenmesini sağlamak
7. Tüm personel üyelerinin çevrimiçi güvenlik rolleri ve sorumlulukları hakkında düzenli, güncel ve uygun eğitim almasını sağlamak ve güvenli, uygun iletişim konusunda rehberlik sağlamak .
8. Çevrimiçi güvenliğin, tüm öğrencilerin yaşa uygun çevrimiçi güvenlik ve ilgili riskler ve güvenli davranışlar hakkında bilgi sahibi olmalarını sağlayan, ilerici bir okul / ortam müfredatı içine yerleştirilmesini sağlamak.
9. Herhangi bir çevrimiçi güvenlik olayından haberdar olmak ve harici ajansların ve desteğin uygun şekilde kullanılmasını sağlamak.
10. İç / yerel ve ulusal destek dahil olmak üzere çevrimiçi güvenlik endişeleriyle ilgili olarak okul / ortam topluluğunun erişebileceği sağlam raporlama kanalları olmasını sağlamak.
11. Cihazların güvenli ve sorumlu kullanımını sağlamak da dahil olmak üzere teknolojinin güvenli kullanımına ilişkin uygun risk değerlendirmelerinin yapılmasını sağlamak.
12. Yönetim Organının bir üyesinin çevrimiçi güvenliği destekleme konusunda öncü bir sorumlulukla tanımlanmasını sağlamak.
13. Güçlü ve iyileştirilmesi gereken alanları belirlemek için mevcut çevrimiçi güvenlik uygulamasını denetlemek ve değerlendirmek.

Okul Müdürünün Kilit Sorumlulukları :

1. Tüm çevrimiçi koruma konularında belirlenmiş bir irtibat noktası olarak hareket etmek ve diğer personel ve diğer kurumlarla uygun şekilde irtibat kurmak .
2. Çevrimiçi güvenliğe ilişkin güncel araştırmaları, mevzuatı ve eğilimleri takip etmek.
3. Olumlu çevrimiçi davranışı teşvik etmek için yerel ve ulusal etkinliklere katılımı koordine etmek. Örneğin Güvenli İnternet Günü (Safe Internet Day)kutlamalarını organize etmek.
4. Çeşitli kanallar ve yaklaşımlarla çevrimiçi güvenliğin öncelikle ebeveynlere, ve sonrasında daha geniş bir topluma kazandırılmasını sağlamak .
5. Uygulamanın yürürlükteki mevzuata uygun olmasını sağlamak için veri koruma ve veri güvenliği için okul lideriyle birlikte çalışmak.
6. Kayıt yapısı ve mekanizmalarını koruyan okulların bir parçası olarak yapılan çevrimiçi güvenlik kaygıları, olayları ve eylemlerinin kaydını tutmak .
7. Eğilimleri belirlemek için okul çevrimiçi güvenlik olaylarını izlemek ve bu verileri, ihtiyacı yansıtacak şekilde okul eğitim yanıtını güncellemek için kullanmak.
8. Çevrimiçi güvenlik kaygıları ve yerel veriler, rakamlar hakkında okul yönetim ekibine, Yönetim Organına ve diğer kurumlara uygun şekilde rapor vermek .
9. Uygun olduğu şekilde yerel ve ulusal organlarla irtibat kurmak .
10. Çevrimiçi güvenlik politikalarını, Kabul Edilebilir Kullanım Politikalarını (AUP'lar) ve diğer ilgili politikaları paydaş girdisi ile düzenli olarak (en az yılda bir kez) gözden geçirmek ve güncellemek için okulla çalışmak, liderlik ve yönetim kurmak.
11. Çevrimiçi güvenliğin diğer uygun okul politikaları ve prosedürleriyle bütünleştirilmesini sağlamak.
12. Tüm paydaş gruplarının, yani ebeveynlerin girdisi olan bir çevrimiçi güvenlik grubuna liderlik etmek.

Tüm Çalışanlarının Temel Sorumlulukları :

1. Çevrimiçi güvenlik politikalarının geliştirilmesine katkıda bulunmak .
2. Okulun Kabul Edilebilir Kullanım Politikalarını (AUP) okumak ve bunlara bağlı kalmak .
3. Okul / ayar sistemleri ve verilerinin güvenliği için sorumluluk almak .
4. Bir dizi farklı çevrimiçi güvenlik meselesi ve bunların bakımlarındaki çocuklarla nasıl ilişkili olabileceğinin farkında olmak .
5. Yeni ve gelişmekte olan teknolojileri kullanırken iyi uygulamaları modellemek
6. Çevrimiçi güvenlik eğitimini mümkün olan her yerde müfredat uygulamasına dahil etmek .
7. İlgilenen bireylerin belirlenmesi ve okulun korunması politika ve prosedürlerini izleyerek uygun önlemleri almak.
8. Çevrimiçi güvenlik konularının içeride ve dışarıda ne zaman ve nasıl yükseltileceğini bilmek .
9. Dahili ve harici olarak çevrimiçi güvenlik sorunları için uygun bir bağlantı noktasına yönlendirme yapabilmek .

10. Sahada ve saha dışında, teknolojiyi kişisel kullanımlarında profesyonel düzeyde bir davranış sürdürmek .
11. Olumlu öğrenme fırsatlarına vurgu yapmak.
12. Bu alanda mesleki gelişim için kişisel sorumluluk alabilmek.

E-Güvenlik Ekibinin Temel Sorumlulukları :

1. Öğrenme fırsatlarının hala en üst düzeye çıkarılmasını sağlarken, güvenli çevrimiçi uygulamaları destekleyen güvenli bir teknik altyapı sağlamak .
2. Liderlik ve yönetim ekibiyle işbirliği içinde sistemlerin ve verilerin güvenliğinin uygulanmasında sorumluluk almak .
3. Okula ait cihazlarda tutulan kişisel ve hassas bilgileri korumak için uygun erişim kontrollerinin ve şifrelemenin uygulanmasını sağlamak .
4. Okul filtreleme politikasının düzenli olarak uygulanmasını ve güncellenmesini ve uygulama sorumluluğunun Belirlenen Koruma Lideri (DSL) ile paylaşılmasını sağlamak.
5. Okul ağının kullanımının düzenli olarak izlenmesini sağlamak ve DSL'ye kasıtlı veya kazayla kötüye kullanımı bildirmek .
6. Herhangi bir ihlali veya endişeyi DSL ve liderlik ekibine bildirmek ve birlikte kaydedildiklerinden ve tavsiye edildiği şekilde uygun önlemlerin alındığından emin olmak.
7. Teknik altyapının güvenliği ilgili olduğu için ilgili mevzuatın incelemek ve anlaşılır kılmak.
8. Özellikle geliştirilmesi ve uygulanmasında, DSL ve liderlik ekibine teknik destek ve perspektif sağlayan uygun çevrimiçi güvenlik politikaları ve prosedürlerini takip etmek.
9. Okulun BİT sisteminin güvenli olduğundan ve yanlış veya kötü niyetli saldırılara açık olmadığından emin olmak.
10. Tüm taşınabilir aygıtlara uygun virüsten koruma yazılımı ve sistem güncellemelerinin yüklendiğinin ve sürdürüldüğünün takibini yapmak .

Öğrencilerin Temel Sorumlulukları:

1. Çevrimiçi güvenlik politikalarının geliştirilmesine katkıda bulunmak .
2. Okul Kabul Edilebilir Kullanım Politikaları (AUP'lar) belirleme ve bunlara uymak .
3. Hem çevrimiçi hem de çevrimdışı ortamlarda başkalarının duygu ve haklarına saygı duymak .
4. Herhangi bir problem yaşadığında güvenilir bir yetişkinden yardım isteme ve çevrimiçi güvenlik sorunları yaşayan diğer kişileri desteklemek .

Öğrenci Velilerinin Temel Sorumlulukları :

1. Okulun Kabul Edilebilir Kullanım Politikaları belirlemek ve bu kurallara uymak.

2. Çevrimiçi güvenlik sorunlarını çocuklarıyla konuşmak, okulu çevrimiçi güvenlik yaklaşımlarında desteklemek ve evde uygun güvenli çevrimiçi davranışları güçlendirmek .
3. Teknolojinin ve sosyal medyanın güvenli ve uygun kullanımları konusunda rol model olmak.
4. Çocuklarının çevrimiçi olarak zarar görme riski taşıdığını gösterebilecek davranış değişikliklerinin belirlenmesi, böyle durumlarla karşılaşıldığında okuldan ve ya uygun kurumlardan yardım ve destek almak.
5. Okul gelişimine katkıda bulunmak, çevrimiçi güvenlik politikaları belirlemek.
6. Öğrenme platformları ve diğer ağ kaynakları gibi okul sistemlerini güvenli ve uygun bir şekilde kullanmak.
7. Yeni ve gelişmekte olan teknolojilerin yarattığı fırsatlar ve risklerle ilgili olarak kendi farkındalık ve öğrenmelerinin sorumluluğunu üstlenmek.

5)TEMEL PRENSİPLER

Kullanım Koşulları

Tüm kullanıcılar okulun bilgisayar sistemlerini kullanarak, okulun söz konusu sistemlerde saklanan veya bu sistemler aracılığıyla gönderilen hiçbir ileti veya verinin gizliliği hakkında herhangi bir beyanda bulunmadığını; okulun bu dokümanda belirtilen haklarını saklı tuttuğunu ve söz konusu sistemlerin kullanımının okul onaylı amaçlar ile sınırlı olduğunu, bu hususta kendilerine gerekli bildirimlerin yapılmış olduğunu kabul ederler. Okulun bilgisayar sistemlerinin Okul faaliyetleri ve önem arz etmeyen konulardaki kişisel kullanımı ile ilişkili olarak kullanılması bir hak değil ancak Okul topluluğunun sınırlı üyelerine tanınan bir ayrıcalıktır. Dolayısıyla, okul dilediği zaman ve herhangi bir bildirimde bulunmaksızın bilgisayar sistemlerinin tamamına veya bir kısmına erişimi (tüm kullanıcılar veya bazı kullanıcılar için) tamamen veya kısmen engelleyebilir. Okulun bilgisayar sistemleri kullanıcıları, işbu Emlakbank Süleyman Demirel Anadolu Lisesi Kabul Edilebilir Kullanım Politikası'na uymak zorundadır ve söz konusu sistemleri kullanarak Kabul Edilebilir Kullanım Politikası'nı kabul etmiş olduklarını ve bunlara uyacaklarını, bu hususta kendilerine bildirim yapılmış olduğunu ve Okulun Kabul Edilebilir Kullanım Politikası'nı uygulamasına izin vermiş olduklarını kabul etmiş olurlar. Kullanıcılar aynı zamanda ilgili mevzuata uyacaklarını ve okulu yükümlülük altına sokacak her türlü davranıştan kaçınacaklarını kabul ederler. Okul, işbu Emlakbank Süleyman Demirel Anadolu Lisesi Kabul Edilebilir Kullanım Politikası ile bilgisayar sistemlerinin kullanımına ilişkin diğer koşulları dilediği zaman önceden herhangi bir bildirimde bulunmaksızın değiştirme hakkını ve ilgili mevzuat gereğince alınması gereken veya alınması uygun olan aksiyonları alma hakkını saklı tutar. Okul, okulun bilgisayar sistemleri ile kullanıcılarının bütünlüğünün söz konusu tesislerin yetkisiz veya uygunsuz kullanımına karşı korunması ve okulun kural ve politikalarının ihlali veya ihlaline neden olacak muhtemel kullanımların tespiti için; herhangi bir bildirimde bulunmaksızın herhangi bir kişinin kullanımını sınırlama veya engelleme ve bir bilgisayar sistemleri için uygun görülen kullanımı zedeleyecek ya da okulun kural veya politikalarının ihlali için kullanılabilecek olan her türlü veri, dosya veya sistem kaynağını

arařtırma, kopyalama, kaldırma veya deęiřtirme hakkını saklı tutar. Emlakbank Sleyman Demirel Anadolu Lisesi bilgisayar sistemlerinin korunması iin sistemlerin periyodik kontrolne iliřkin hakları ve dięer her trl hakkını saklı tutar. Okula ait bilgisayarlarda, akıllı tahtalarda, sunucularda, okul sunucularında iřlenen e-posta mesajlarında zararlı yazılım taraması sistemleri koruma amalı yapılacak kontrollere rnektir.

6)EVİRİMİ İLETİřİM VE DAHA GVENLİ TEKNOLOJİ KULLANIMI İİN EMLAKBANK SLEYMAN DEMİREL ANADOLU LİSESİ AęLARININ YNETİLMESİ

Okul Web Sitesinin Ynetilmesi:

1. Web sitesinde iletiřim bilgileri okul adresi, e-posta ve telefon numarası olacaktır. Personel veya ğrencilerin kiřisel bilgileri yayınlanmayacaktır.
2. Okul Mdr yayınlanan evrimii ierik iin genel yayın sorumluluęunu alacak ve bilgilerin doęru ve uygun olmasını saęlayacaktır.
3. Web sitesi, eriřilebilirlik fikri mlkiyet haklarına saygı, gizlilik politikaları ve telif hakkı da dahil olmak zere okulun yayın ynergelerine uyacaktır.
4. Spam maillerden korunmak iin e-posta adresleri evrimii olarak dikkatli bir řekilde yayınlanacaktır.
5. ğrenci alıřmaları ğrencilerin izniyle ya da ebeveynlerinin izniyle yayınlanacaktır.
6. Okul web sitesinin ynetici hesabı, uygun bir řekilde gl řifreyle řifrelenerek korunacaktır.
7. Okul, evrimii gvenlik dahil olmak zere, toplumun yeleri iin okul web sitesinde korunma hakkında bilgi gnderecektir.

evrimii Grnt ve Videolar Yayınlama

1. Okul, evrimii paylařılan tm resimlerin ve videoların okul resim kullanımı politikasına uygun řekilde kullanılmasını saęlayacaktır.
2. Okul , resimlerin ve videoların tmnn, veri gvenlięi, Kabul Edilebilir Kullanım Politikaları, Davranıř Kuralları, sosyal medya, kiřisel cihazların ve cep telefonlarının kullanımı gibi dięer politikalar ve prosedrlere uygun řekilde yer almasını saęlayacaktır.
3. Grnt politikasına uygun olarak, ğrencilerin resimlerinin / videolarının elektronik olarak yayınlanmasından nce her zaman ebeveynlerin yazılı izni alınacaktır.

Kiřisel Cihaz ve Cep Telefonlarının Kullanımı

1. Cep telefonlarının ve ocukların, genlerin ve yetiřkinler arasındaki dięer kiřisel cihazların yaygın bir řekilde sahiplenilmesi, tm yelerin cep telefonlarının ve kiřisel cihazların sorumlu bir řekilde kullanılmasını saęlamak iin gerekli adımları atmalarını gerektirir.
2. ocukların, Genlerin ve yetiřkinlerin cep telefonlarının ve dięer kiřisel cihazların kullanımı, okul tarafından kararlařtırılacak ve okul Kabul Edilebilir Kullanım veya Cep Telefonu Politikası dahil olmak zere uygun politikalarda yer alacaktır.

3. Emlakbank Süleyman Demirel 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

1. Öğrenciler, kişisel cihazların ve cep telefonlarının güvenli ve uygun kullanımı konusunda eğitim alacaklardır.
2. 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 bulundurmamak kesinlikle yasaktır.
3. Öğrenciler ders başlamadan önce telefonlarını okul yönetimi tarafından sınıflarda yaptırılan telefon kutularına koymakla yükümlüdür.
4. Cep telefonunun amacı dışında kullanımı ihlali olduğunda, 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.
5. 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.
6. Çocukların cep telefonlarını veya kişisel cihazlarını eğitim etkinliğinde kullanımı, okul idaresi tarafından onaylandığında gerçekleşecektir.
7. Bir öğrenci ebeveynlerini arama gereği duyduğunda, okul telefonunu kullanmasına izin verilecektir.
8. Ebeveynlerin okul saatlerinde cep telefonu ile çocuklarıyla iletişim kurmamaları, okul idaresine başvurmaları önerilir. İstisnai durumlarda öğretmenin onayladığı şekilde istisnalara izin verilebilir.
9. Öğrenciler, telefon numaralarını yalnızca güvenilir arkadaşlarına ve aile üyelerine vermelidirler.
10. Öğrencilere, cep telefonlarının ve kişisel cihazların güvenli ve uygun bir şekilde kullanımı öğretilecek ve sınırların ve sonuçların farkına varılacaktır.
11. 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.

Ziyaretçi Kişisel Cihazlar ve Cep Telefonlarının Kullanımı

1. Ebeveynler ve ziyaretçiler, okulun kabul edilebilir kullanım politikasına

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

Çevrimiçi Fotoğraf ve Videoların Kullanımı

1. Çevrimiçi olarak paylaşılan tüm resim ve videoların okul resim kullanımı politikasına uygun olarak kullanılması sağlanacaktır.
2. Görüntü politikası doğrultusunda, öğrencilerin görüntüleri, videoları elektronik olarak yayınlanmadan önce her zaman velilerden yazılı izin alınacaktır.

E-Postayı Yönetme

1. Zincir e-postaların vb. iletilmesine izin verilmez. Spam veya önemsiz postalar engellenip, e-posta sağlayıcısına bildirilecektir.
2. Veri koruma mevzuatına tabi olabilecek herhangi bir içerik(örn. Hassas veya kişisel bilgiler) içeren elektronik iletişim yalnızca güvenli ve şifreli e-posta kullanılarak gönderilecektir.
3. Okul e-posta sistemlerine erişim her zaman veri koruma mevzuatına ve gizlilik gibi diğer uygun okul politikalarına uygun olarak gerçekleşecektir.
4. Topluluğun üyeleri, saldırgan bir iletişim alırlarsa, görevlendirilen bir personele derhal bildirecektir.
5. Okul e-posta adresleri ve diğer resmi iletişim bilgileri kişisel sosyal medya hesapları oluşturmak için kullanılmayacaktır.

Eğitim Amaçlı Resmi Video Konferans ve Web Kamerası Kullanımı

1. Tüm video konferans ekipmanı, kullanılmadığında ve uygun olduğunda otomatik cevaplamaya ayarlanmadığında kapatılacaktır.
2. Harici IP adresleri başka siteler tarafından kullanılamaz.
3. Video konferans iletişim bilgileri herkese açık olarak yayınlanmayacaktır.
4. Video oluşturma ekipmanı güvenli bir şekilde saklanacak ve gerekirse kullanılmadığında kilitlenecektir.
5. Okul video konferans ekipmanı izinsiz okul binalarından çıkarılmayacaktır.
6. Personel, harici video konferans fırsatlarının veya araçlarının uygun şekilde risk değerlendirmesini sağlayacak ve etkinliklere erişmek için kullanılan hesapların ve sistemlerin uygun şekilde güvenli ve emniyetli olmasını sağlayacaktır.

Video Konferans Kullanımında Kullanıcılar

1. Öğrenciler, video konferans görüşmesi veya mesajı yapmadan veya cevaplamadan önce öğretmenden izin ister.
2. Video konferans, öğrencilerin yaşı ve yeteneği için uygun şekilde denetlenecektir.

3. Video konferans faaliyetlerine katılan çocuklar öncesinde velilerin onayı alınacaktır.
4. Video konferans, sağlam bir risk değerlendirmesinin ardından resmi ve onaylı iletişim kanalları aracılığıyla gerçekleştirilecektir.
5. Video konferans yönetim alanlarına veya uzaktan kumanda sayfalarına yalnızca yöneticilere erişim izni verilecektir.
6. Eğitici video konferans hizmetleri için benzersiz oturum açma ve şifre ayrıntıları yalnızca personel üyelerine gönderilecek ve güvenli tutulacaktır.

Video Konferansın İçeriği

1. Bir video konferans dersi kaydedilirken, tüm siteler ve katılımcılar tarafından yazılı izin verilecektir. Konferansın başlangıcında kaydın nedeni verilmeli ve video konferansın kaydedilmesi tüm taraflara açık olmalıdır. Kaydedilen malzeme güvenli bir şekilde saklanacaktır.
2. Üçüncü taraf materyalleri dahil edilecekse, okul üçüncü şahısların fikri mülkiyet haklarını ihlal etmemek için kaydın kabul edilebilir olduğunu kontrol edecektir.
3. Okul, bir video konferansa katılmadan önce diğer konferans katılımcılarıyla iletişim kuracaktır. Eğer okul dışı bir siteyse, okul sınıfa uygun malzeme sağlayıp sağlamadığını kontrol edecektir.

Genel Sosyal Medya Kullanımı

1. Topluluğunun tüm üyeleri, sosyal medyaya her zaman olumlu, güvenli ve sorumlu bir şekilde katılmaya teşvik edilecektir.
2. Sosyal medyanın güvenli ve sorumlu kullanımı ile ilgili bilgiler okulun tüm üyelerine açık ve düzenli olarak iletilecektir.
3. Okul saatleri boyunca sosyal ağ uygulamalarının kişisel kullanım için kullanımına izin verilir veya izin verilmez. Uygunsa, örneğin belirli zamanlarda izin verildiğinde veya açık izinle beklentileri eklenir. Bu, öğrencilerin yaşına, yeteneğine ve personelin erişimine bağlı olarak değişecektir. Sorumlu öğretmen tarafından karar verilir.

7) GÖZDEN GEÇİRME

Bu dokümanı gözden geçirme ve güncelleştirme sorumluluğu okul e-güvenlik ekibine aittir. Yapılan değişiklik ve güncellemeler idare onayıyla yayınlanır. Gözden geçirme ve güncelleştirme yılda en az bir kez (gerekli görüldüğü takdirde daha fazla) yapılır.

E Güvenlik Ekibi:

Fatma Nurlu ŞAHİN - Müdür Yardımcısı

Özge YILDIRIM - Bilişim Teknolojileri Öğretmeni

Fatma AKSAKAL - İngilizce Öğretmeni

Fatma Sibel OKTAY - Rehber Öğretmen