AKŞEMSEDDİN İLKOKULU
E-GÜVENLİK OKUL POLİTİKASI veKURALLARI

AMAÇ:

- Akşemseddin İlkokulu olarak, bilişim teknolojilerinin günlük yaşamdaki vazgeçilmez öneminin farkında olmak. Yaşamımızdan çıkaramayacağımız bu teknolojilerin güvenli ve bilinçli bir şekilde kullanıldığında bizleri çok daha ileri seviyelere taşıyacağının zorunluluk olduğunun önemini kavramak. Amacımız e-güvenlik çalışmaları ile internet, bilgisayar, diz üstü bilgisayar ve cep telefonlarını kullanırken; öğrencilerin, velilerin ve öğretmenlerin korunması ve bu teknolojileri bilinçli bir şekilde kullanması.
- İnternetin ve teknolojinin yaşamın önemli bir parçası olması sebebiyle, herkes, riskleri yönetme ve strateji geliştirme yöntemlerinin öğrenilmesi konusunda bilinçlendirilmelidir.
- Politikamız, yöneticiler, öğretmenler, veliler, tüm personel ve öğrenciler için hazırlanmış olup, internet erişimi ve bilgi iletişim cihazlarının kullanımı için geçerlidir.

SORUMLULUKLAR:

- E-güvenlik politikalarının gelişmesine katkıda bulunmak.
- Olumlu öğrenme aşamasında mesleki gelişim için sorumluluk almak.
- Okul ve içerisindekileri korumak için e-güvenlik konusunda sorumluluk almak.
- Teknolojiyi güvenli ve sorumlu kullanmak. Zarar görülmesi durumunda tehlikeyi gözlemleyip ilgili birimlere iletmek.

OKUL WEB SİTESİ:

- Akşemseddin İlkokulu olarak websitemizde okulumuzun adres, telefon, fax ve e-posta adres bilgileri bulunmaktadır.
- Sitemizde yayınlanan tüm içerikler okul müdürümüzün onayından geçtikten sonra siteye konulmaktadır.
- Okulumuzun web sitesi Okul Web Yönetim ekibinin sorumluluğunda olup güvenlik önlemleri alınmış durumdadır. Okul websitesinin yönetici hesabı, uygun bir şekilde güçlü şifreyle şifrelenerek korunacaktır.

- Öğrenci çalışmaları, etkinlikler ile ilgili resimler velilerinin izinleriyle yayınlanmaktadır.

GÖRÜNTÜ VE VİDEOLARIN PAYLAŞIMI:

- Paylaşılan tüm fotoğraf ve videolar okul politikasına uygun şekilde okul idaresinin izni ve onayı ile paylaşılmaktadır.
- Öğrenci içerikli tüm paylaşımlarda velilerin izinleri alınmaktadır.
- Veli izni yanında öğrencinin de izni olmadan fotoğrafı veya video çekilip kullanılmamaktadır.

KULLANICILAR:

- Okul idaresi tarafından görevli kılınanlar haricindeki kişiler tarafından, okul ve okul bahçesi sınırları içerisinde fotoğraf ve video çekimi yapılamaz.
- Bir öğrencinin diğer bir öğrencinin fotoğraf ve videosunu çekmek istemesi durumunda da idareden ve öğrenciden izin alması gerekmektedir.
- Paylaşılan öğrencilerimizin bulunduğu etkinliklerde, etkinlik öncesinde velilerin izinleri alınmaktadır.
- Kullanıcılar, şahsi sosyal medya hesaplarında, okul öğrencileri ve çalışanlarının yer aldığı görselleri, okul yetkili mercileri tarafından onaylanmadan paylaşamazlar.

İÇERİK:

- Okul öğrenci ve çalışanlarını ilgilendiren tüm içerik, ancak kontrol ve onay süreçlerinden geçtikten sonra, paylaşıma açık hale gelecektir.
- Öğretmenlerimizin okul sitesinde paylaşmak istedikleri içerik Web yayın ekibi ve okul idaresinin onayından geçtikten sonra yayınlanmaktadır.
- Okul görevlileri tarafından yayınlanan resim ve videolarda öğrencilerin kişisel bilgilerine kesinlikle yer verilmez.

İNTERNETİN VE BİLİŞİM CİHAZLARININ GÜVENLİ KULLANIMI:

- İnternet; bilgiye ulaşmakta en önemli araçlardan biri, bunu okuldaki müfredat ile ilişkilendirerek doğru bilgiye en güvenli şekilde öğrencilerimizi ve öğretmenlerimizi ulaştırabilmek için elimizden gelen çabayı gösteriyoruz.
- İnternet erişimlerimiz MEB tarafından öğrencilerimizin yaşına uygun olarak filtrelenmektedir.
- Tüm okulumuza ait bilişim cihazlarımızı kullanım politikamıza uygun şekilde güvenli hale getirmiş durumdayız.
- Tüm çalışanlarımız, velilerimiz ve öğrencilerimiz etkili ve verimli çevrimiçi materyallerin kullanımı konusunda bilgilendirilmiştir.
- E-güvenlik ve siber zorbalık konuları müfredatla ilişkilendirilerek derslerde işlenmektedir. Rehberlik öğretmenlerimiz yıllık planlarına dahil edip, bu konularda yıl içinde öğrencilere bilgi aktarımı yapılmaktadır.
- Çevrimiçi materyaller öğretme ve öğrenmenin önemli bir parçası olup müfredat içinde aktif olarak kullanılmaktadır ve öğrencilerin derse katılımını artırmaktadır.
- Güvenli internet günü okulumuzda kutlanmaktadır. Hafta boyunca seminerler, tanıtıcı afişler ve panolarla etkin katılım sağlanmaktadır.

Daha Güvenli İnternet Merkezi (gim.org.tr) - Safer Internet Center'ın resmi sayfası. http://guvenlinet.org.tr/tr/

Güvenli Web (guvenliweb.org.tr) - çevrimiçi güvenlik konuları için farkındalık portalı.

Güvenli Çocuk (guvenlicocuk.org.tr) - 13 yaşından küçük çocuklar için oyun ve eğlence portalı.

Ihbar Web (ihbarweb.org.tr) - yasadışı içerik için telefon hattı.

İnternet BTK (internet.btk.gov.tr) - İnternet ve BT yasası konusunda farkındalık portalı.

SID Page (gig.org.tr) - Daha Güvenli İnternet Günü Türkiye'de resmi sayfası. Veli ve öğrencilere tanıtılmış buralardaki eğitici ebeveyn ve öğrenci bilgilendirici vidoları ,sunuları izlenmiştir.

Okulumuz 5651 yasasına uygun güvenlik prosedürlerini tamamen uygulamaktadır. Okulumuzda cihazların internete bağlanabilmesi için MEB tarafından hazırlanan sertifika yüklenmesi gerekmektedir. Bu da internete bağlanan cihazların çevrimiçi faaliyetlerinin denetlenmesini sağlamaktadır.

EBA CANLIDERSLERDE E- GÜVENLİK

- EBA portal üzerinden yaptığımız canlı ders ara yüzlerinde her öğrenci derse sadece ismi yazılı olarak katılır.
- İsimlerini kendilerinin değiştirmelerine izin verilmez.
- Derse girişlerde bekleme odası aktiftir.
- Toplantı ID ve şifresi üçüncü şahıslarla paylaşılmaz
- Senkron ve asenkron derslerde öğrencilere paylaşılan çizgi film,ders içeriği safe.youtube(video link) adresinden filtrelenerek reklamsız ve zararlı içeriklerden arındırılarak paylaşılır.

CEP TELEFONLARI VE KİŞİSEL CİHAZLARIN KULLANIMI:

- Okul saatleri içinde öğrencilerimizin kişisel cep telefonu kullanımı yasaktır.
- Her türlü kişisel cihazların sorumluluğu kişinin kendisine aittir.
- Okulumuz bu tür cihazların kullanımından doğacak olumsuz sağlık ve yasal sorumlulukları kabul etmez.
- Okulumuz kişisel cep telefonlarının ve bilişim cihazlarının kayıp, çalınma ve hasardan korunması için gerekli tüm önlemleri alır fakat sorumluluk öğrenci ve velisine aittir.
- Okulumuz öğrencileri, velilerini aramaları gerektiği durumlarda okula ait olan telefonları bir okul idarecisi veya rehber öğretmen gözetiminde kullanabilirler.
- Öğrencilerimiz eğitim amaçlı (web 2 araçlarının kullanımı vb) kişisel cihazlarını kullanmak için okul yönetiminden izin almalıdır.
- Velilerimiz okul saatleri içerisinde öğrencileriyle görüşme yapmamaları gerektiği konusunda bilgilendirilirler. Eğer zorunlu haller var ise okul yönetiminden izin alarak görüşme yapmaları sağlanmalıdır.
- Öğrencilerimiz cep telefon numaralarını yalnızca güvenilir kişilerle paylaşmaları, tanımadıkları güvenilir bulmadıkları kişilerle cep telefonu gibi kişisel bilgilerini paylaşmamaları gerektiği konusunda bilinçlendirilmektedirler.
- Çalışanlar (öğretmen, idareci, personel vb) kişisel cep telefonlarını ders saatlerinde sessize alarak yada kapatarak görevlerine devam etmelidir.
- Kurum çalışanları (öğretmen, idareci, personel vb) ve öğrenciler sosyal medya ya da sohbet programları üzerinden öğrenci ya da kurum çalışanlarından gelecek olan ya da kendilerinin gönderecekleri her türlü içerik ve mesajlaşmanın hukuki sorumluluğunu taşımaktadır, uygunsuz olabilecek her türlü içerik ve mesajlaşma ivedilikle okul yönetimi ile paylaşılır. Böyle bir duruma mahal vermemek için gereken önlemler alınır.

E-GÜVENLİK EĞİTİMİ:

- Çevrimiçi güvenlik (e-Güvenlik) politikası, tüm çalışanların katılımı için resmi olarak sağlanacak ve tartışılacak ve korunma sorumluluğumuzun bir parçası olarak güçlendirilecek ve vurgulanacaktır.
- Öğrenciler için e-güvenlik müfredatı ilgili derslerin özellikle bilişim teknolojileri dersinin yıllık planlarına eklenerek öğrenciler bu konularda bilgilendirilir.
- Tüm kullanıcıların internet kullanımları okul idaremiz tarafından takip edilmektedir. Bu bilgi tüm kullanıcılara iletilmiştir.
- Öğrencilerimizin ihtiyaçları doğrultusunda çevrimiçi güvenliği geliştirmek için rehberlik öğretmenleri akran eğitimi uygulamaktadır.
- Çevrimiçi güvenlik politikası tüm çalışanlarımıza resmi olarak duyurulacaktır.
- Güvenli internet günü okulumuzda kutlanmaktadır. Bu güne yönelik okul koridorları ve sınıflarda pano çalışmalarımız ve sosyal medya paylaşımlarımız olur.

ÇEVRİMİÇİ OLAYLAR VE KORUMA:

- Okulumuzun tüm üyeleri çevrimiçi riskler konusunda bilgilendirilecektir. Eğitimler yapılıp içerikler açıklanacaktır.
- Okulumuzda yasadışı içerik, güvenlik ihlali, siber zorbalık, cinsel içerikli mesajlaşma, çocuk istismarı, kişisel bilgi güvenliği gibi konularda bilgilendirme çalışmaları yapılmaktadır.
- Güvenli internet günü kutlanarak okulumuzda farkındalık oluşturulmaktadır.
- Okulumuzda internet, bilgi teknolojileri ve ekipmanlarının yanlış kullanımı ile ilgili tüm şikayetler Rehber Öğretmenimiz tarafından okul müdürüne bildirilecektir.
- Okulumuzun tüm üyeleri gizlilik ve güvenlik endişelerini ortadan kaldırmak için resmi okul kurallarına uygun şekilde davranmaları hususunda bilgilendirilir.

Akşemseddin İlkokulu için Gönül ŞAHİN tarafından sunulan eylem planı - 26.01.2021 @ 09:06:15

Doldurulmuş Değerlendirme Formunuzu e-Güvenlik Etiketi portalına göndererek, okulunuzdaki e-Güvenlik durumunu analiz etme yolunda önemli bir adım attınız. Tebrikler! Okulunuzda e-Güvenliği daha da geliştirmek için neler yapabileceğinizi görmek için lütfen Eylem Planınızı dikkatlice okuyun. Eylem Planı, 3 temel alana bölünmüş yararlı tavsiyeler ve yorumlar sunar: altyapı, politika ve uygulama.

Altyapı

Teknik Güvenlik

- Her yaştan öğrencide bir eğitim yaklaşımı ve dayanıklılık oluşturmak da güvenli ve sorumlu çevrimiçi kullanımın anahtarıdır, bu nedenle tüm öğretmenleri öğrencileriyle iyi ve güvenli bir dijital vatandaş olma konusunda nasıl konuşacakları konusunda bir tartışma yapmak için bir araya getirin. Rol yapma ve grup oyunları yoluyla bu konu hakkında sınıfta gerçekleştirilebilecek tartışma örnekleri için www.europa.eu/youth/EU_en adresini ziyaret edin.

- Okul sisteminiz bir güvenlik duvarı ile korunmaktadır. Güvenlik duvarının sağlanması ve yönetiminin, gerektiği zaman düzenli olarak gözden geçirildiğinden ve güncellendiğinden emin olun.

Öğrenci ve personelin teknolojiye erişimi

- Personelin ve öğrencilerin izninizi takiben okulunuzda USB bellekleri kullanmalarına izin verilmesi gerçeği, ilgili tüm personelin güvenli bir şekilde kullanılabileceklerini bilmeleri için yeterli eğitim almalarını gerektirecektir. Durum bu mu? Personel ve öğrencilere izin verirken sistemlerinizi güvende tutmak için ayrıca Kabul Edilebilir Kullanım Politikanıza temel kuralları da eklemeniz gerekir. Tüm güvenlik hususlarını kapsadığınızdan emin olmak için www.esafetylabel.eu/group/community/use-of-removable-devices adresindeki çıkarılabilir cihazların kullanımı hakkındaki bilgi formunu kontrol edin.

- Mobil cihazları yasaklamanın amaca uygun bir kural olup olmadığını ve okulunuzun bazı sınıf etkinlikleri için dijital cihazlara izin vermek isteyip istemediğini düşünün. Kabul Edilebilir Kullanım Politikanızın bir parçası olarak, dijital teknolojilerin sınıfta nasıl kullanılabileceği ve kullanılamayacağına dair bir bölüm geliştirebilirsiniz. Okulda Cep Telefonlarını Kullanma hakkındaki bilgi formuna (www.esafetylabel.eu/group/community/using-mobile-device-in-schools) adresinden bakın.

Veri koruması

- Okulunuzdaki sistem tarafından tüm kullanıcılara farklı bir şifre atanması iyidir. Tüm okul üyelerine kendilerine verilen şifreyi hiçbir yere, kesinlikle bilgisayardaki bir çıkartmanın üzerine yazmamalarını hatırlatın. Ayrıca, Kabul Edilebilir Kullanım Politikasının personele ve öğrencilere şifrelerini güvende tutmalarını ve başkalarıyla paylaşmamalarını hatırlatmasını sağladığından emin olun.

- Öğrenci verilerini şifreleme ve güvenli bir şekilde saklama konusunda iyi bir politikanız var. Tüm yeni personelin şifreleme ve veri işleme prosedürlerinden haberdar olduğundan ve okulunuz için veri denetleyicisi olarak görev yapan adlandırılmış bir iletişim noktası olduğundan emin olun. Hassas verileri bir şifreleme sistemi aracılığıyla korumaya ilişkin bazı yönergeleri okul profilinize yükleyin. Böylece diğer okullar deneyimlerinizden faydalanabilir.

Yazılım lisanslama

- Tüm personelin yeni yazılım satın alma prosedüründen haberdar olduğundan ve tüm lisansların onları kullanacak öğrenci ve personel sayısına uygun olduğundan emin olun. Wikipedia'daki Son kullanıcı lisans sözleşmesi bölümü(End-user license agreement) hüküm ve koşulları anlamak ve yazılım sözleşmelerini karşılaştırmak için yararlı bilgiler sağlayacaktır.

- Sorumlu personelin kurulu yazılım ve bunların lisans durumlarından tamamen haberdar olması iyi bir uygulamadır.

BT(Bilişim Teknolojileri) yönetimi

- Okul bilgisayarlarına yüklenen yeni yazılımın kullanımı konusunda eğitim almanız ve / veya rehberlik etmeniz iyi bir uygulamadır. Bu, okul üyelerinin yeni özelliklerden yararlanmasını ve aynı zamanda ilgili yerlerde güvenlik ve veri koruma sorunlarının farkında olmalarını sağlar.

- BİT(Bilişim ve İletişim Teknolojileri) ağından sorumlu kişinin, okulun sahip olduğu donanımda hangi yazılımın bulunduğundan tam olarak haberdar olmasını sağlamak iyi bir uygulamadır ve bu, Okul Politikası ve Kabul Edilebilir Kullanım Politikası'nda açıkça belirtilmelidir. Ağdan sorumlu kişinin, lisans gereksinimlerine uyumu ve bu yeni yazılım ağın çalışmasını engellemeyeceğini garanti edebilmesi gerekir.

Politika

Kabul Edilebilir Kullanım Politikası

- Okul politikaları ve prosedürleri, bir okul içinde sorunsuz bir işlem sağlamak ve tüm okul üyelerinin aynı kurallar ve yönergelere uyması için gereklidir. Okul politikalarının var olduğundan ve tüm okul üyelerinin bunlardan haberdar olduğundan emin olun. Bununla ilgili daha fazla bilgiyi e-Güvenlik Etiketi(eSafety Label) web sitesinde bulabilirsiniz.

- Okulunuzda her değişiklik yapıldığında, okul politikalarının gerekirse revize edilmesi iyi bir uygulamadır. Bununla birlikte, okul dışındaki değişikliklerin de yeni yasalar veya değişen teknolojiler gibi politikaları etkileyebileceğini unutmayın. Bu nedenle, lütfen politikalarınızı en az yılda bir kez gözden geçirin.

Raporlama ve Olay Yönetimi

- Bununla ilgili açıkça iletilmiş bir Okul Politikasına sahip olmak önemlidir ve Kabul Edilebilir Kullanım Politikasında da belirtilmelidir. Potansiyel olarak yasa dışı olarak değerlendirilenler kişiden kişiye değişebilir, bu nedenle bunun personel üyeleriyle tartışılması ve okul standartlarının belirlenmesi önemlidir. Öğrenciler ve öğretmenler dahil olmak üzere okulun tüm üyeleri onlardan haberdar edilmeli ve onlara saygı duymaları istenmelidir.

- Öğretmenleriniz (siber) zorbalığı nasıl tanıyacaklarını ve üstleneceklerini biliyor. Öğrenciler ve ebeveynler arasında da farkındalık yaratmanın yollarını düşünün. Daha fazla bilgi için e-Güvenlik bilgi formuna bakın.

- Okul dışında meydana gelen çevrimiçi sorunlar, kaçınılmaz olarak okul içinde de etkili olacaktır. Okulun, Okul Politikası ve Kabul Edilebilir Kullanım Politikasında bu tür sorunların nasıl ele alınacağına dair bir açıklama yapması gerekip gerekmediğini değerlendirin. Okulların birbirlerinin stratejilerini paylaşmasına ve onlardan öğrenmesine olanak sağladığından, Olayları ele alma formunda (www.esafetylabel.eu/group/teacher/incident-handling) olayları isimsiz olarak belgelemeyi unutmayın.

- Öğretmenler potansiyel olarak yasa dışı materyallerle başa çıkma konusunda eğitim aldı mı? Prosedür, tüm öğretmenlerin ve öğrencilerin imzaladığı Okul Politikası ve Kabul Edilebilir Kullanım Politikasında açıkça belirtilmiş mi? Tüm personel ve öğrenciler, yasadışı olduğundan şüphelenilen içeriği ulusal INHOPE yardım hattına (www.inhope.org) bildirmeleri gerektiğinin farkında olmalıdır.

Personel politikası

- Akıllı telefonlar veya diğer mobil cihazlar gibi yeni teknolojiler, beraberinde bir dizi yeni risk getirir. Öğretmenlerinizin bunların farkında olmasını sağlayın. Bu şekilde, cihazları kullanırken tehlikelerden kaçınabilir ve ayrıca bilgiyi öğrencilere aktarabilirler.

Öğrenci uygulaması/davranışı

- Öğrenciler için elektronik iletişim yönergeleri Kabul Edilebilir Kullanım Politikasında açıkça belirtilmelidir. Okul çapında standartlar belirlenmezse öğrenciler arasındaki iletişim hızla bozulabilir ve bu da siber zorbalık gibi olaylara yol açar. Etkili ve sorumlu iletişim hakkında bilgi edinmek, her genç için gerekli bir yeterlilik olduğundan okul müfredatının bir parçası olmalıdır. Uygulamak istediğiniz standartları tanımlamak için bunu bir personel toplantısında tartışın.

- E-Güvenlik hakkında tartışırken, okulunuzdaki öğrenciler bazen faaliyetler hakkında geri bildirimde bulunabilir. Mümkün olduğunca onları dahil edin, böylece öğretmenin gerçek yaşam sorunlarını fark etmesini sağlayın.

Çevrimiçi okul varlığı

- Okulunuzun çevrimiçi bir varlığı olsa da, öğrenciler onu şekillendirmeye katılamazlar. Belki bir dijital konseyin parçası olarak öğrencileri dahil etmenin bir yolu olup olmadığını araştırın. Medya okuryazarlığı ve ilgili konular hakkında bilgi edinmek için harika bir fırsat. Aynı zamanda bir akran destek ağının kurulmasına da yardımcı olabilir. E-Güvenlik Etiketi bilgi formu hakkında daha fazla bilgi edinin.

Uygulama

E-Güvenlik Yönetimi

- E-Güvenlik sorunları için irtibat sağlayan bir yönetici veya yönetim kurulu üyesi atamayı düşünün. Ayrıca Okul Politikanızı gözden geçirirken, e-Güvenlik olaylarının sayısı ve türü hakkında yıllık olarak yönetim organına bildirmeyi de düşünün. Okul Politikası ile ilgili bilgi formumuza bakın www.esafetylabel.eu/group/community/school-policy.

- E-Güvenlik'ten okulunuzdaki tüm personelin sorumlu olması iyidir. Ancak, ihtiyaç duyulan odağı sağlamak için e-Güvenlik konularından genel olarak sorumlu olacak bir kişinin atanması iyi bir uygulamadır. İdeal olan, kıdemli liderlik ekibinden biri olmasıdır. Bu kişinin Okul Politikanızın geliştirilmesine ve düzenli olarak gözden geçirilmesine dâhil olmasını sağlayın. Bu kişi sadece

bilgilendirilmekle kalmamalı, aynı zamanda www.esafetylabel.eu/group/teacher/incident-handling adresinde bir olay ortaya çıktığında Olay ele alma formunu da doldurmalıdır.

Müfredatta e-Güvenlik

- Öğrencilerin teknolojiyi nasıl kullandıklarına bağlı olarak farklı mesajlara ihtiyaç duyacaklarını göz önünde bulundurarak, mevcut tüm kaynakları tam olarak kullanarak e-Güvenlik müfredatının ortaya çıkan sorunlara ayak uydurmasını sağlayın ve önceki öğrenmeye dayalı olmasını sağlayın.

- Tüm öğrencilerin bir miktar e-Güvenlik eğitimi alması gerekir. Öğrenciler okul içinde teknolojiyi kullanmasalar da, muhtemelen evde kullanacaklardır. Ve bu nedenle, çevrimiçi teknolojinin kullanımını çevreleyen bazı sorunların ele alınması gerekiyor.

- E-Güvenlik'in okulunuzda müfredatın bir parçası olarak öğretilmesi iyidir. Tüm personelin, yalnızca BİT (Bilişim ve İletişim Teknolojileri) veya Kişisel Sosyal ve Sağlık dersleri yoluyla değil, müfredat boyunca uygun olan yerlerde e-Güvenlik eğitimi vermesini sağlayın. Siz / personeliniz, www.esafetylabel.eu/group/community/embedding-online-safety-in-curriculum adresindeki müfredata e-Güvenlik Yerleştirme bilgi sayfasında bazı yararlı fikirler ve kaynaklar bulabilirsiniz.

Müfredat dışı etkinlikler

- Güvenli İnternet Günü'nü, tüm okul topluluğunun çevrimiçi güvenlikle ilgilenmesini sağlayacak bir mekanizma olarak kullanın. www.saferinternetday.org adresinde bulunan bilgi ve kaynaklar, akran savunuculuk faaliyetlerini teşvik etmek için ideal bir fırsat sunmaktadır.

- Öğrencileri akran rehberliğine dâhil etmeye çalışın ve onlara düşüncelerini ve anlayışlarını akranlarıyla paylaşmaları için fırsatlar sağlayın. Ayrıca, daha fazla fikir ve kaynak almak için e-Güvenlik Etiketi portalının kaynak bölümüne (resource section) bakın.

- İstendiğinde müfredat zamanı dışında öğrencilerinize e-Güvenlik desteği sağlamanız iyidir. Çevrimiçi güvenlik sorunları ile başa çıkmak için tüm öğrencilere destek sunmayı düşünün. Öğrencilerin Facebook gizliliklerini vb. ayarlamalarına yardımcı olmak için bir "operasyon" sağlamak faydalı olabilir. E-Güvenlik Etiketi portalı, bunun için yararlı olacak kaynakları sağlar. Öğrencilerin okul dışında çevrimiçi teknolojiyi kullanmasıyla ilgili bilgi formunu www.esafetylabel.eu/group/community/pupils-use-of-online-technology-out-school adresinde inceleyin.

Destek kaynakları

- Okulunuzda, öğrencilerin e-Güvenlik danışmanları olmaya aktif olarak teşvik edilmesi harika. Bu ağı güçlendirmeye yönelik yaklaşımınızı, forum veya okulunuzun profil sayfası aracılığıyla e-Güvenlik Etiketi web sitesinde diğer öğretmenlerle paylaşmak isteyebilirsiniz, böylece başkaları da onu kopyalayabilir.

- Okulunuzda e-Güvenlik konularında eğitilmemiş bir okul danışmanı var. Yeni medya ile ilgili konularda öğrencilere yardımcı olmak için daha donanımlı olmak üzere bu öğretmenin izleyebileceği bir eğitim kursu olup olmadığını araştırın.

Personel eğitimi

Gönderdiğiniz Değerlendirme Formu büyük bir soru havuzundan oluşturulmuştur. Ankette belirtilmeyen alanlarda e-Güvenliği iyileştirip iyileştirmediğinizi bilmek de bizim için ayrıca yararlıdır. Bu tür değişikliklerin kanıtını e-Güvenlik Portalının **Okul Alanım(My School Area)** bölümünden **Kanıt Yükle(Upload Evidence)** yoluyla yükleyebilirsiniz. Unutmayın, Değerlendirme Formunun doldurulması Akreditasyon Sürecinin yalnızca bir parçasıdır, çünkü kanıtların yüklenmesi, **Forum** aracılığıyla başkalarıyla görüşmeleriniz ve sağlanan şablonda **olayları raporlanmanız** da hesaba katılır.

eSafety Label - Action Plan

Action plan submitted by Gönül ŞAHİN for Akşemseddin İlkokulu - 26.01.2021 @ 09:06:15

By submitting your completed Assessment Form to the eSafety Label portal you have taken an important step towards analysing the status of eSafety in your school. Congratulations! Please read through your Action Plan carefully to see what you can do to improve eSafety further in your school. The Action Plan offers useful advice and comments, broken down into 3 key areas: infrastructure, policy and practice.

Infrastructure

Technical security

- An educational approach and building resilience in pupils of all ages is also key to safe and responsible online use so bring together all teachers to have a discussion on how they will talk to their pupils about being a good and safe digital citizen. See www.europa.eu/youth/EU_en for examples of discussions that can take place in the classroom on this topic, through role-play and group games.

- Your school system is protected by a firewall. Ensure that the provision and management of the firewall are regularly reviewed and updated, as and when required.

Pupil and staff access to technology

- The fact that staff and pupils are allowed to use USB memory sticks in your school following permission, would require that all staff concerned receive adequate training to be able to know when they can be used safely. Is this the case? To keep your systems secure whilst allowing staff and pupils you also need to include the ground rules in your Acceptable Use Policy. Check the fact sheet on Use of removable devices at www.esafetylabel.eu/group/community/use-of-removable-devices to make sure you cover all security aspects.

- Consider whether banning mobile devices is a rule that is fit for purpose and if your school might want to allow digital devices for some class activities.You could develop as part of your Acceptable Use Policy a section on how digital technologies can and cannot be used in the classroom; see the fact sheet on Using Mobile Phones at School (www.esafetylabel.eu/group/community/using-mobile-device-in-schools).

Data protection

- It is good that all users are attributed a different password by the system in your school. Remind all school members never to write their given password down anywhere, certainly not on a sticker on a computer! Also, ensure that the Acceptable Use Policy reminds staff and pupils to keep their passwords secure and not share them with others.

- You have a good policy of encrypting pupil data and storing it safely. Ensure all new staff made aware of the procedures for encryption and data handling and that there is a named point of contact acting as the data

controller for your school. Upload to your school profile some guidelines about protecting sensitive data through an encryption system so that other schools can benefit from your experience.

Software licensing

- Ensure that all staff are aware of the procedure for purchasing new software and that all licenses are appropriate for the number of pupils and staff that will be using them. The End-user license agreement section in Wikipedia will provide useful information for understanding terms and conditions and comparing software agreements.

- It is good practise that the member of staff responsible is fully aware of installed software and their license status.

IT Management

- It is good practise that your are training and/or providing guidance in the use of new software that is installed on school computers. This ensures that school members will take advantage of new features, but also that they are aware of security and data protection issues where relevant.

- It is good practice to ensure that the person in charge of the ICT network is fully informed of what software is on school-owned hardware and this should be clearly indicated in the School Policy and the Acceptable Use Policy. The person responsible for the network needs to be able to guarantee conformity with licensing requirements and that new software won't interfere with network operation.

Policy

Acceptable Use Policy (AUP)

- School policies and procedures are essential to ensure a smooth operation within a school and that all school members follow the same set of rules and guidelines. Ensure that school policies exist and that all school members are aware of them. You can find more information on this in the of the eSafety Label website.

- It is good practise that whenever changes are put into place in your school, the school policies are revised if needed. Note though, that also changes outside the school can affect policies such as new legislations or changing technologies. Therefore please review your policies at least annually.

Reporting and Incident-Handling

- It is important to have a clearly communicated School Policy on this, and it should be mentioned in the Acceptable Use Policy too. What is considered to be potentially illegal can vary from person to person, so it is important that this is discussed with staff members and that school standards are set. All members of the school including pupils and teachers must be informed of them and required to respect them.

- Your teachers know how to recognise and handle (cyber)bullying. Think about ways to raise awareness also among pupils and parents. Check out the eSafety fact sheet for more information.

- Online issues that take place outside of school will inevitably have an impact inside school. Consider whether the school needs to make a statement about how such issues will be dealt with in the School Policy and the Acceptable Use Policy. Don't forget to anonymously document incidents on the Incident handling form

(www.esafetylabel.eu/group/teacher/incident-handling), as this enables schools to share and learn from each other's strategies.

- Have teachers received training on dealing with potentially illegal material? Is the procedure clearly indicated in the School Policy and the Acceptable Use Policy which all teachers and pupils have signed? All staff and pupils should be aware that they should report any suspected illegal content to the national INHOPE hotline (www.inhope.org).

Staff policy

- New technologies, such as smartphones or other mobile devices bring a new set of risks with them. Ensure that your teachers are aware of those. This way they can avoid the pitfalls when using the devices and also pass the knowledge onto the pupils.

Pupil practice/behaviour

- Electronic communication guidelines for pupils should be clearly communicated in the Acceptable Use Policy. Communication between pupils can rapidly degenerate if school-wide standards are not set, giving rise to incidents such as cyberbullying. Learning about effective, responsible communication should also be part of the school curriculum, as it is a necessary competence for every young person. Discuss this at a staff meeting in order to define the standards you want to implement.

- When discussing eSafety pupils at your school can sometimes provide feedback on the activities . Involve them as much as possible so that the teacher recognises real life issues while the pupils are more engaged.

School presence online

- While your school has an online presence, pupils cannot take part in shaping it. Explore if there could be a way to involve pupils, maybe as part of a digital council. It's a great opportunity to learn about media literacy and related issues. It also can help to establish a peer network of support. Find out more about in the eSafety Label fact sheet.

Practice

Management of eSafety

- Consider appointing a governor or board member who provides a liaison for eSafety issues. Consider also reporting on the number and type of eSafety incidents to the governing body on an annual basis when you also review your School Policy. See our fact sheet on School Policy www.esafetylabel.eu/group/community/school-policy.

- It is good that all staff in your school are responsible for eSafety. However, it is good practice to appoint a person who will have overall responsibility for eSafety issues to provide the focus needed. Ideally this should be someone from the senior leadership team. Ensure that this person is involved in the development and regular review of your School Policy. She or he should not only be informed, but should also fill out the Incident handling form whenever an incident arises at www.esafetylabel.eu/group/teacher/incident-handling.

eSafety in the curriculum

- Ensure that the eSafety curriculum keeps up with emerging issues by making full use of all available resources and ensure that it builds on prior learning, bearing in mind that pupils will need different messages depending on how they are using the technology.

- All pupils need to receive some eSafety education. Although pupils may not be using technology within school, they will more than likely be using it at home and so some of the issues surrounding the use of online technology need to be addressed.

- It is good that eSafety is taught as part of the curriculum in your school. Ensure that all staff are delivering eSafety education where appropriate throughout the curriculum and not just through ICT or Personal Social and Health lessons. You/your staff may find some useful ideas and resources in the fact sheet Embedding eSafety in the curriculum at www.esafetylabel.eu/group/community/embedding-online-safety-in-curriculum.

Extra curricular activities

- Use Safer Internet Day as a mechanism to get the whole school community involved with online safety. The information and resources available at www.saferinternetday.org offer an ideal opportunity to promote peer advocacy activities.

- Try to engage pupils in peer mentoring and provide them with opportunities to share their thoughts and understanding with their peers. Also check out the resource section of the eSafety Label portal to get further ideas and resources.

- It is good that you provide eSafety support for your pupils outside curriculum time when asked. Consider offering all pupils support to deal with online safety issues. It may be helpful to provide a “surgery" to help pupils to set their Facebook privacy etc. The eSafety Label portal provides resources that will be useful for this; check out the fact sheet on Pupils' use of online technology outside school at www.esafetylabel.eu/group/community/pupils-use-of-online-technology-outside-school.

Sources of support

- It is great that in your school pupils are actively encouraged to become eSafety mentors. You might want to share your approach to strengthening this network with other teachers on the eSafety Label website via the forum or your school's profile page, so that others can replicate it.

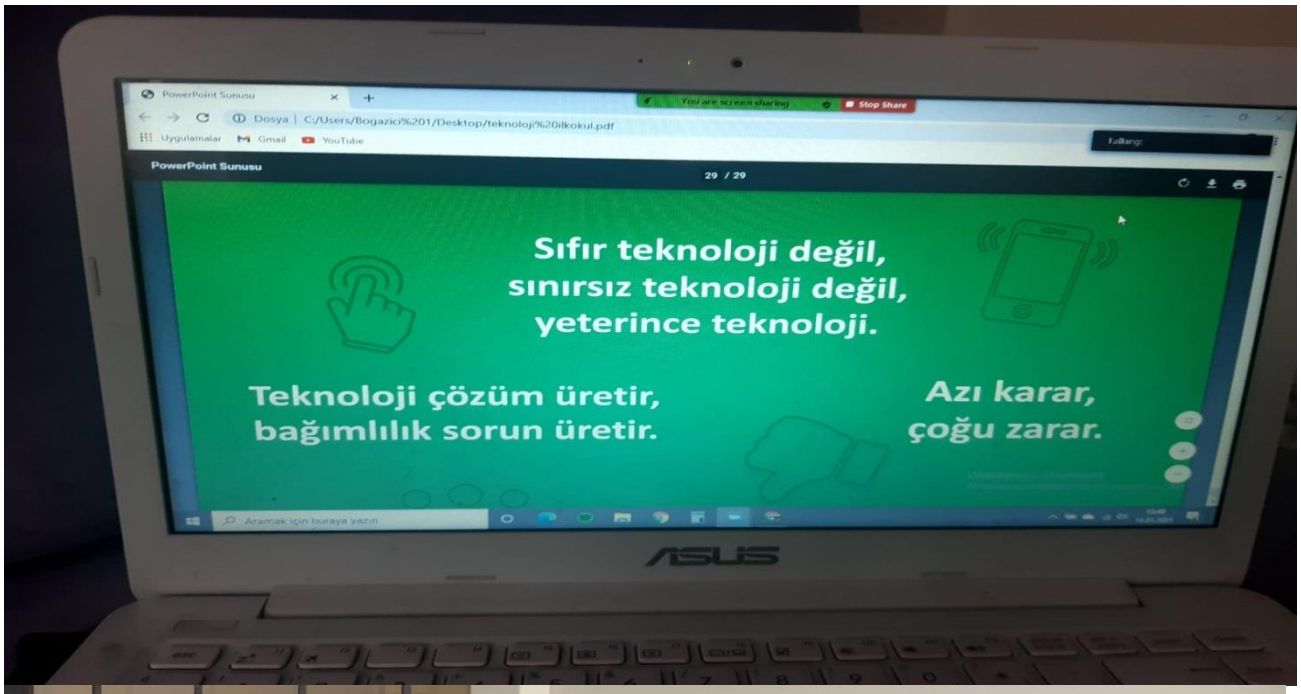
- There is a school counselor in your school though not trained on eSafety issues. Investigate if there is a training course that this teacher could follow in order to be better equipped to help pupils dealing with issues related to new media.

Staff training

The Assessment Form you submitted is generated from a large pool of questions. It is also useful for us to know if you are improving eSafety in areas not mentioned in the questionnaire. You can

upload evidence of such changes via the **Upload evidence** on the **My school area** section of the eSafety Portal. Remember, the completion of the Assessment Form is just one part of the Accreditation Process, because the upload of evidence, your exchanges with others via the **Forum**, and your **reporting of incidents** on the template provided are all also taken into account.


ÇIKIŞ
Uygulama
Talimatına
Dikkat Edin
Kişisel
Bilgilerinizi
Paylaşmayın
1-A
3/F


PowerPoint Sunusu
Dosya | C:/Users/Bogazici%201/Desktop/teknoloji%20ilkokul.pdf
Uygulamalar
Gmail
YouTube
You are screen sharing
Stop Share
PowerPoint Sunusu
29 / 29
Sıfır teknoloji değil,
sınırsız teknoloji değil,
yeterince teknoloji.
Teknoloji çözüm üretir,
bağımlılık sorun üretir.
Azı karar,
çoğu zarar.
Aramak için buraya yazın
ASUS

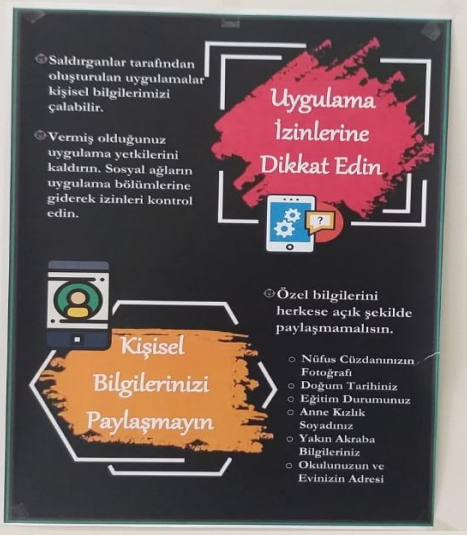

TAŞINABİLİR AYGIT KULLANAMAZ


OKULUMUZ ÖĞRENCİLERİ İZİNSİZ CEP TELEFONU
ve
TAŞINABİLİR AYGIT KULLANAMAZ
ELİNİZİ YAKLAŞTIRIN
SAĞLIK ELİNİZDE


Milli Eğitim Bakanlığımızın protokollerine
Avrupa komisyonu Safety hareket eylem planına göre
KULUMUZ ÖĞRENCİLERİ İZİNSİZ CEP TELEFONU
ve
TAŞINABİLİR AYGIT KULLANAMAZ
AKŞEMSEDDİN


AKTİF
DİKKAT!
KAYGAN
ZEMİN


İstiklal Marşı


Saldırganlar tarafından oluşturulan uygulamalar kişisel bilgilerimizi çalabilir.
Vermiş olduğunuz uygulama yetkilerini kaldırın. Sosyal ağların uygulama bölümlerine giderek izinleri kontrol edin.
Uygulama İzinlerine Dikkat Edin
Kişisel Bilgilerinizi Paylaşmayın
Özel bilgilerini herkese açık şekilde paylaşmamalısın.
Nüfus Cüzdanınızın Fotoğrafı
Doğum Tarihiniz
Eğitim Durumunuz
Anne Kızlık Soyadınız
Yakın Akraba Bilgileriniz
Okulunuzun ve Evinizin Adresi


Milli Eğitim Bakanlığımızın protokollerine,
Avrupa komisyonu eSafety hareket eylem planımıza göre
OKULUMUZ ÖĞRENCİLERİ İZİNSİZ CEP TELEFONU
ve
TAŞINABİLİR AYGIT KULLANAMAZ
12:45
T.C. MİLLİ EĞİTİM BAKANLIĞI

T.C.
SELÇUKLU KAYMAKAMLIĞI
Akşemseddin İlkokulu Müdürlüğü

Sayı : 77887655-50.99-E.11024088 21.08.2020
Konu : Öğretmenler Kurulu Toplantısı

AKŞEMSEDDİN İLKOKULU ÖĞRETMENLERİNE

Okulumuz 2020 - 2021 Eğitim - Öğretim yılı sene başı öğretmenler kurulu toplantısı 24.08.2020 tarihinde saat 11.00 'de aşağıdaki gündem maddeleri ile okul müdürü Memili OFLAZ başkanlığında yapılacaktır. Okulumuz idareci ve öğretmenlerinin belirtilen saatte okulumuzda hazır bulunmaları hususunda;

Gereğini önemle rica ederim.

Memili OFLAZ
Okul Müdürü

GÜNDEM:
1-Açılış ve yoklama
2-Saygı duruşu ve İstiklâl Marşı.
3-Öğretmenler Kurulu yazmanlığına 2 asil 2 yedek üye seçimi.
4-Salgın sürecinde eğitim öğretim faaliyetleri,bu süreçte alınması gereken önlemler ve uyulması gereken kurallarla ilgili açıklamaların yapılması
5-Okul öncesi ve ilköğretim okulu yönetmeliği ile ilgili bilgilendirme. Ders planları, öğretim programları ile ilgili açıklamalar.
6-"Öğretmen Strateji Belgesi" hakkında bilgilendirme.(Milli Eğitim Bakanlığı-Öğretmen Yetiştirme ve Geliştirme Genel Müdürlüğü)
7-"Bakanlığımız 2023 vizyonu ile ilgili açıklamalar.
8-Milli bayram törenleri,belirli gün ve haftalarla ilgili görevlendirmeler.İdareci görev dağılımı ile ilgili açıklamalar.
9-Öğretmen-öğrenci-veli ilişkileri. Veli toplantıları ve tarihlerinin belirlenmesi.
10-Öğretmen nöbet hizmetinin gerektirdiği sorumluluklar ve görevler.
11-Bayrak Törenleri Yönergesine göre nöbetçi öğretmenlerin yapacağı iş ve işlemler.
12-Günlük zaman çizelgesi; toplanma giriş-çıkışlar ve öğretmen devam-devamsızlıkları.
13-Öğrenci devam takip işleri, ders defterlerinin işlenmesi, Nöbet Defterinin işlenmesi ile ilgili açıklamalar.
14- Ders araç-gereçleri, bakımı temizliği, kullanılması
15-Sınıf kitaplıkları ve bununla ilgili yapılacak iş ve işlemler:Kitaplık demirbaş defteri, Okuma ile ilgili yapılacak etkinliklerin planlanması.
16-Okul Rehberlik Kurulunun oluşturulması ve çalışmalarının değerlendirilmesi.
17-Okulumuz Stratejik Planı ile ilgili görev alanları ve komisyonların çalışmaları
18-İki, üç ve dördüncü sınıflarda branş öğretmenlerinin girdiği ders saatlerinde görevlendirme Okuma yazma bilmeyen öğrencilerle ilgili yapılacak çalışmalar.
19-Egzersiz çalışmaları ve destek eğitim odası ile ilgili açıklamalar
20-Okul Çalışma Takviminin ve Öğretmen Çalışma takvimlerinin oluşturulması hakkında bilgilendirme.
21-Okul koridorlarındaki panoların Sosyal Kulüplerce Sosyal Etkinlikler Yönetmeliğine göre düzenlenmesi.Yazı İnceleme Kuruluna imzalatılması arşivlenmesi, İnternet güvenliği(e-Güvenlik) ile ilgili çalışmaların planlanması.
22-Tasarruf tedbirlerinde, bütün öğretmenlerin su, elektrik, ısınma vb. gibi hususlara dikkat etmesi, öğrencileri bu yönde yönlendirmesi.
23-Serbest Etkinlikler Saati uygulamaları sırasında yapılacak çalışmalar.Değerler eğitim ile ilişkilendirme.SEDEP çalışmaları ile ilgili açıklamalar ve ekiplerin oluşturulması.
24-Sınıfların öğretmenlere dağılımı ve sabahçı öğlenci tespiti. Okul zümre başkanlarının belirlenmesi.Zümre toplantı tarih ve saati hakkında bilgilendirme.
25-15 Temmuz Demokrasi Zaferi ve Şehitleri Anma Etkinlikleri Programı (18-22 Eylül 2019) kapsamında yapılacak faaliyetleri ile ilgili görevlendirme yapılması.

26-İlköğretim Haftası Kutlamaları görevlendirilmesi
27-Sosyal Etkinlikler Yönetmeliği çerçevesinde yıl içerisinde yapılacak kermeslerin tarihlerinin belirlenmesi.Sosyal ve kültürel faaliyetler ile ilgili açıklamalar..
28-Anasınıfı ile ilgili iş ve işlemler.
29-Sosyal kulüplerin dağılımı
30-Okul Aile Birliği denetim kuruluna 2 asil ve 2 yedek öğretmen üye seçimi
31-Resmi yazı ve e-postalar ile ilgili açıklamalar.
32-Okullarda kurulması zorunlu olan kurullara öğretmen seçimi:
A- Taşınır Mal Satın Alma Komisyonu
B- Taşınır Mal Muayene Kabul Komisyonu
C- Sosyal Etkinlikler Kurulu
D- Rehberlik Hizmetleri Yürütme Komisyonu,Bep Biriminin Kurulması.
E- Okul Gelişimi Toplam Kalite Yönetim Ekibi
F- Demokrasi Eğitimi Ve Okul Meclisi
G- Okul Aile Birliği Yönetim Kuruluna Üye Seçimi
H- Yayın,yazı İnceleme Kurulu
J-Bep Biriminin Kurulması.
K-Okul Web Sitesi Güncelleme Ve Yazılarını İnceleme Komisyonu
L- Taşınır Mal Sayım Düşüm Komisyonu
M-proje kurulu oluşturulması
33-Dilek ve temenniler.
34-Kapanış.

TUTANAKTIR

Akşemseddin İlkokulu Anasınıfı, 1. Sınıf , 2. Sınıf, 3.Sınıf ve 4. Sınıf öğrencilerine uzaktan eğitim sürecinde 01.12.2020-31.12.2020 tarihleri arasında **GÜVENLİ İNTERNET KULLANIMI VE TEKNOLOJİ BAĞIMLILIĞI** konulu bilgilendirme çalışması okulumuz rehberlik servisi tarafından gerçekleştirilmiştir. Ayrıca EBA üzerinden oluşturulan rehberlik gurubunda da konu ile ilgili etkinlik çalışmaları öğrencilerle paylaşılmıştır. 04.01.2021

Nursel TUTAL YÜCE
Rehber Öğretmen

Servet GÜDÜCÜ
Rehber Öğretmen

Ebru CİNGÖZ
Rehber Öğretmen

Hasan YILDIRIM
Müdür Yardımcısı