Beypazarı Şehit Mehmet Çifci İmam Hatip Ortaokulu Egüvenlik Eylem Planı

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.

Öğrenci ve personelin teknolojiye erişimi

Okulunuzdaki bilgisayar laboratuvarlarında yer ayırtmak zor. Bunun kolaylaştırılıp kolaylaştırılamayacağını ve / veya bir ders içinde yeni medyanın kullanımını kolaylaştırmanın başka yolları olup olmadığını araştırın. Dijital cihazları kullanmak, yeni teknolojilerin sorumlu bir şekilde kullanımını öğrencilere öğretmenin en iyi yoludur. Bir BYOD (kendi cihazınızı getirin) yaklaşımının işe yarayıp yaramayacağını düşünün.

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 nasıl kullanılabileceği ve kullanılamayacağına dair bir bölüm geliştirebilirsiniz. sınıf; Okulda Cep Telefonlarını Kullanma hakkındaki bilgi sayfasına bakın (www.esafetylabel.eu/group/community/using-mobile-device-in-schools).

Personel ve öğrenciler okul ağınızda kendi ekipmanlarını kullanabildikleri için, Kabul Edilebilir Kullanım Politikasının okulun tüm üyeleri tarafından düzenli olarak gözden geçirildiğinden ve gerektiği şekilde uyarlandığından emin olmak önemlidir. Her akademik yılın başında öğrencilerle tartışılmalıdır, böylece onları ve mahremiyetlerini korumak için neyin mevcut olduğunu ve nedenini anlasınlar. Politikayı teknolojiden çok davranışa dayandırın. Ziyaretçiler ayrıca okulun ağını kullanmadan önce Kabul Edilebilir Kullanım Politikasını okuyup imzalamalıdır.

Veri koruması

E-posta sisteminizin korunması ve öğrenci verilerinin yerinde aktarılması için bir politikanızın olması iyidir. Bu bağlamda, tüm personelin okul makinelerinde uygunsuz veya yasa dışı içerik keşfettiklerinde ne yapacakları konusunda net olmaları için yönergeler hazırlamak önemlidir. Daha fazla bilgi için Hassas verilerin korunması hakkındaki bilgi sayfasına bakın (www.esafetylabel.eu/group/community/protecting-sensitive-data-in-schools).

Okulunuzun, özellikle taşınabilir cihazlar olmak üzere cihazların korunmasının önemi konusunda eğitim materyalleri sağlaması iyidir. Lütfen bunları giriş yoluyla başkalarıyla paylaşmayı düşünün. Ayrıca, malzemelerinizin en son teknoloji ile uyumlu olduğundan emin olmak için düzenli olarak gözden geçirildiğinden emin olun.

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, hüküm ve koşulları anlamak ve yazılım sözleşmelerini karşılaştırmak için yararlı bilgiler sağlayacaktır.

Yeni yazılımın kurulumu için sahip olduğunuz etkili süreçler hakkında tüm yeni personele bilgi verilmesini sağlamak önemlidir. Bu, sistemlerinizin güvenliğinin korunabileceği ve personelin öğretme ve öğrenmeye yardımcı olacak yeni yazılım uygulamalarını deneyebileceği anlamına gelir.

Okulunuz, yazılım ihtiyaçları için gerçekçi bir bütçe belirledi. Bu iyi. Bu şekilde kalmasını sağlayın. Alternatiflere de bakmak isteyebilirsiniz, ör. Bulut hizmetleri veya açık yazılım.

BT yönetimi

Okulunuzda, herhangi bir personelin yeni donanım / yazılım için talepte bulunmasına izin veren bir mekanizma vardır - bu, makul bir süre içinde bilinçli bir karara götüren bir taleptir. Bu harika, çünkü öğretmen okul politikasına uymaya devam ederken yeni teknolojilerden yararlanabilir.

Politika

Kabul Edilebilir Kullanım Politikası (AUP),

Amaca uygun olduğundan ve okul genelinde tutarlı bir şekilde uygulandığından emin olmak için Cep Telefonu Politikasını düzenli olarak gözden geçirin. Okulda cep telefonu kullanımı (www.esafetylabel.eu/group/community/using-mobile-device-in-schools) ve Okul Politikası www.esafetylabel.eu/group/community/school-policy) hakkındaki bilgi sayfaları yardımcı bilgi.

Raporlama ve Olay Yönetimi

Yeni personel de dahil olmak üzere tüm personelin, bir okul makinesinde uygunsuz veya yasadışı materyal bulunursa ne yapılacağına ilişkin yönergelerden haberdar olmasını sağlayın. Politikanın titizlikle uygulandığından da emin olun. Okulun kıdemli liderlik ekibinin bir üyesi bunu izlemelidir.

Tüm personel, potansiyel olarak yasa dışı olabilecek materyallerle ilgilenme prosedürüne aşina mı? Bu tür bir vakada genel sorumluluk alan okul kıdemli liderlik ekibinden belirlenmiş bir kişi var mı? Prosedürün Okul Politikasında tüm personele ve Kabul Edilebilir Kullanım Politikasında personel ve öğrencilere açıkça bildirilmesi gerekir. Yasadışı olduğundan şüphelenilen içeriği ulusal INHOPE yardım hattınıza (www.inhope.org) bildirmeyi unutmayın.

Lütfen bu sorunları ele aldığınız materyalleri özellikle e-Güvenlik Etiketi portalındaki öğrenciler ve ebeveynlerle paylaşın.

Avrupa genelindeki okullardan, sizin ve başkalarının gelecekte kullanabileceği başarılı olay yönetimi uygulamalarının bir veri tabanı oluşturmaya katkıda bulunduğunuz için okulunuzda meydana gelen siber zorbalık olaylarını merkezi olarak kaydetmek iyi bir uygulamadır. Öğrencilerin Kabul Edilebilir Kullanım Politikanızdaki zorbalıkla mücadele yönergelerine kaydolmalarını sağlayın.

Personel politikası

Okul politikasının akıllı telefonlar gibi potansiyel olarak güvenli olmayan cihazlarla ilgili riskler hakkında bilgi içermesi ve buna atıfta bulunulması iyi bir uygulamadır. Okul politikanızı, Okulum alanından da erişilebilen kanıt yükleme aracı aracılığıyla paylaşmayı düşünün.

Okulunuzda kullanıcı hesapları zamanında yönetilir. Kötüye kullanım riskini azalttığı için bu önemlidir.

Öğrenci alıştırması / davranışı

Okulunuzun, öğrenci davranışları için olumlu ve olumsuz sonuçlara dair okul çapında bir yaklaşımı vardır. Bu iyi bir uygulamadır, lütfen politikanızı e-Güvenlik portalının Okulum alanı aracılığıyla paylaşın, böylece diğer okullar da ondan öğrenebilir.

Kabul Edilebilir Kullanım Politikanızda elektronik iletişim yönergeleri tanımladınız ve bu, diğer okullar için yararlı bir iyi uygulama örneği olacaktır. Öğrenciler için elektronik iletişim kuralları hakkında bir öğretici oluşturabilir ve diğer okulların deneyimlerinizden yararlanabilmesi için Okul alanınız üzerinden okul profilinize yükleyebilir misiniz?

Çevrimiçi okul varlığı

Okulunuzun çevrimiçi itibarını izlemeye kendini adamış bir kişi var ve bu iyi bir uygulamadır. Düzenli bir aramayla hemen görünmeyebilecek yeni sitelerin her zaman farkında olun. En son sitelerden haberdar olun ve bunları periyodik olarak izleyin çünkü olumsuz bir bakış açısına sahiplerse okullara, öğrencilerine ve personeline özellikle zarar verebilirler.

Uygulama

Müfredatta eSafety eSafety yönetimi

Ortaya çıkan sorunlara ayak uyduran bir e-Güvenlik müfredatı sağlayabilmeniz övgüye değer. Kullanılabilir hale getirildikçe yeni kaynakları kullanmaya devam edin. Okul profilinize müfredatı nasıl tasarladığınıza ve kullandığınız kaynakların bazılarına bağlantılara ilişkin bir taslak yükleyebilir misiniz - bu, diğer okullar için çok yararlı olacaktır.

Cinsiyet yazımının okul genelinde daha geniş çevrimiçi güvenlik eğitimine entegre edilmesi iyi bir şey. Bu eğitimin etkisini değerlendirebiliyor musunuz? Öğrencilerin davranışlarını değiştirmelerine yardımcı olur mu? Nereden biliyorsunuz?

Çocuk koruma politikanız içinde cinsel mesajlaşmaya belirli bir atıfta bulunmanız iyi bir şey çünkü bu, birçok gencin uğraşmak zorunda kaldığı büyüyen bir sorun. Bu konuda öğrencilere uygun eğitimi vermeniz de önemlidir.

Ülkenizde yasal bir zorunluluk olup olmadığına bakılmaksızın e-Güvenlik'in tüm müfredata dahil edilmesi gerekir. Bunu destekleyecek, ücretsiz olarak temin edilebilen çok iyi birkaç çalışma planı vardır; Daha fazla bilgi için e-Güvenliği müfredata yerleştirme bilgi sayfasına bakın:

www.esafetylabel.eu/group/community/embedding-online-safety-in-curriculum.

Müfredat dışı etkinlikler

E-Güvenlik konusunda öğrenciler arasında akran danışmanlığını nasıl düzenlersiniz? ENABLE projesinin kaynaklarına göz atın ve fikirlerinizi eSafety Label topluluğu forumunda paylaşın, böylece diğer okullar da benzer bir yaklaşım oluşturmak için deneyimlerinizden yararlanabilir.

Ulusal Güvenli İnternet Merkezinizdeki çevrimiçi e-Güvenlik kaynaklarını sık sık kullandığınızı bilmekte fayda var. Bu kaynakları okulunuzda yararlı buldunuz mu? Lütfen kullanımları ve değerleriyle ilgili geri bildiriminizi şu adrese gönderin: info-insafe@eun.org.

ESafety Label topluluğu aracılığıyla öğrencilerinizin çevrimiçi alışkanlıkları hakkında sahip olduğunuz bilgileri diğer okullarla paylaşmayı düşünün. Örneğin, öğrencilerin çevrimiçi alışkanlıkları hakkındaki en son anket bulgularınızı Okulum alanınız aracılığıyla okul profilinize yükleyebilirsiniz.

Destek kaynakları

Öğrencilere güven öğretmeni olarak hareket eden, e Güvenlik konularında bilgili bir personele sahip olmanız harika.

Ebeveynlerden kendilerine sağlanan e-Güvenlik desteğinin türü hakkında geri bildirim isteyin ve bunlardan yararlanan ve bunlara erişen ebeveynlerin sayısını en üst düzeye çıkarmak için yenilikçi yollar düşünün. Ebeveynlere iletilebilecek kaynaklar ve ebeveyn akşamları için fikirler bulmak için www.esafetylabel.eu/group/community/information-for-parents adresindeki Ebeveynler için bilgiler bilgi sayfasına bakın.

Personel eğitimi

Öğretmenlere boş zamanlarında öğrenciler tarafından kullanılan teknoloji hakkında bilgi vermeniz iyi bir uygulamadır. Bu önemlidir, çünkü bu farkındalık, okulun gücünün kapatılması meselesini ele almanın ilk adımıdır. Aynı zamanda, öğrencilerden okul dışında kendileri için mevcut olmayan teknolojiyi kullanarak ödevlerini yapmaları istenmemelidir. Okullarda Essie BİT Anketi'ne bir göz atmak isteyebilirsiniz