e-Güvenlik Etiketi - Eylem Planı

Çayırkent Çok Programlı Anadolu Lisesi için Niyazi Gürgen tarafından sunulan eylem planı - 22.12.2020 @ 14:43:19

Doldurulmuş değerlendirme formunuzu güvenlik etiketi portalına göndererek okulunuzdaki güvenlik durumunu analiz etmek için önemli bir adımı tamamladınız. Tebrikler. Lütfen
e-Güvenliğinizi daha da iyileştirmek için neler yapabileceğinizi görmek için Eylem Planınızı dikkatlice okuyun. Okul Eylem Planı, 3 temel alana bölünmüş yararlı ipuçları ve yorumlar sunar: altyapı, politika ve uygulama.

Altyapı

Teknik güvenlik

- ICT hizmetlerinizin düzenli olarak gözden geçirilmesi, güncellenmesi ve artık kullanılmıyorsa kaldırılması iyi bir uygulamadır.

- Okul sisteminiz bir güvenlik duvarı ile korunmaktadır. Güvenlik duvarının sağlanmasının ve yönetiminin gerektiği şekilde ve gerektiğinde düzenli olarak gözden geçirildiğinden ve güncellendiğinden emin olun.

Öğrenci ve personelin teknolojiye erişimi

- Okulunuzda bilgisayar laboratuvarlarının kolayca rezerve edilebilmesi iyidir. Diğer dijital cihazları derslere entegre etme seçeneğini düşünün, çünkü bunları kullanmak, yeni medyayla ilgilenirken öğrenciler için en iyi uygulamayı sağlar. Güvenlik konularının da tartışıldığından emin olun.

- Tüm personel ve öğrencilerin okulunuzdaki USB bellekleri kullanmasına izin verilir. Bu iyi bir uygulamadır ve Kabul Edilebilir Kullanım Politikanız, tüm çıkarılabilir medyanın okul sistemlerinde kullanılmadan önce kontrol edilmesini şart koşmalıdır. Tüm güvenlik hususlarını kapsadığınızdan emin olmak için www.esafetylabel.eu/group/community/use-of-removabledevices adresindeki çıkarılabilir cihazların kullanımı hakkındaki bilgi formunu kontrol edin.

- Cep telefonlarına ilişkin politikanın okul genelinde tutarlı bir şekilde uygulanmasını sağlayın. Şu linke bir göz atın Okulda Cep Telefonlarının Kullanımı hakkında bilgi sayfası (www.esafetylabel.eu/group/community/using-mobile-device-inschools).

Veri koruması

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

- Okulunuz için, belirli okul kayıtlarının nasıl saklandığını, arşivlendiğini ve imha edildiğini ayrıntılı olarak anlatan bir saklama planı vardır. Bu çok iyi. Planın izlendiğinden emin olun

ve Veri Koruma Yasası ve diğer ilgili mevzuatla ilgili olmasını sağlamak için düzenli olarak gözden geçirin. Daha fazla bilgi için ilgili bilgi formunu kontrol edin.

Yazılım lisanslama

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

BT yönetimi

Politika

Kabul Edilebilir Kullanım Politikası (AUP)

- Diğer okul politikaları gözden geçirilirken, e-Güvenlik'in kapsadığı çok çeşitli konuları göz önünde bulundurarak e-Güvenlik'e atıfta bulunmanın uygun olup olmayacağını düşünün.

Raporlama ve Olay Yönetimi

- 'Okul dışında meydana gelen çevrimiçi olaylara' ilişkin politikayı daha açık hale getirin ve Okul Politikası ve Kabul Edilebilir Kullanım Politikası aracılığıyla herkese açıkça iletilmesini sağlayın. Okulların birbirlerinin stratejilerini paylaşmasına ve onlardan öğrenmesine olanak sağladığından, Olayları ele alma formunda (www.esafetylabel.eu/group/teacher/incidenthandling) olayları isimsiz olarak belgelemeyi unutmayın.
- Öğretmenleriniz (siber) zorbalığı nasıl tanıyacaklarını ve üstleneceklerini bilir. Öğrenciler ve ebeveynler arasında da farkındalık yaratmanın yollarını düşünün. Daha fazla bilgi için e-Güvenlik bilgi formuna göz atın.
- 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 açık bir şekilde iletilmesi gerekir. Yasadışı olduğundan şüphelenilen içeriği ulusal INHOPE yardım hattınıza bildirmeyi unutmayın. (www.inhope.org)

Personel politikası

- Yeni personel de dahil olmak üzere tüm personelin çevrimiçi davranışa ilişkin politikadan haberdar olmasını sağlayın. Bu, personel toplantılarında düzenli olarak tartışılan ve Okul Politikasında ve Kabul Edilebilir Kullanım Politikasında personel ve

öğrencilere açıkça iletilen bir konu olmalıdır. Her iki belgeyi de gerektiği gibi düzenli olarak inceleyin ve güncelleyin.

Öğrenci alıştırması / davranışı

- Öğrencilerin, e-Güvenlik konusunu tartışırken, günlük yaşamlarında olup bitenlere dayalı olarak, müfredat dışı ve müfredat dışı olsun, okul etkinliklerini şekillendirme olanağına sahip olmaları iyidir. Bu şekilde daha meşgul olacaklar ve öğretmenin gerçek yaşam sorunlarını tanımasına da olanak tanıyor.

- 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, sorumlu iletişim hakkında bilgi edinmek de eğitimin bir parçası olmalıdır. Okul müfredatı, her genç için gerekli bir yeterliliktir. Uygulamak istediğiniz standartları tanımlamak için bunu bir personel toplantısında tartışın.

- 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.

Çevrimiçi okul varlığı

- Öğrencilerin, ebeveynlerin ve personelin fotoğraflarını çekmeye ilişkin politikayı gözden geçirin ve son gelişmeleri yansıtıp yansıtmadığını kontrol edin. İdeal olarak, politika belirli teknolojiler yerine davranışa odaklanmalıdır. Okulda fotoğraf ve video çekme ve yayınlama hakkındaki bilgi sayfası (www.esafetylabel.eu/group/community/taking-andpublishing-photos-and-videos-at-school) iyi bir başlangıç noktası sağlayacaktır.

- Öğrencilerin okulun çevrimiçi varlığı hakkında geri bildirim vermesi iyidir. Tamamen öğrenciler tarafından yönetilen bir alan yaratmayı düşünün. Medya okuryazarlığı ve ilgili konular hakkında bilgi edinmek için harika bir fırsat. Aynı zamanda bir eş destek ağının kurulmasına da yardımcı olabilir. E-Güvenlik Etiketi bilgi formunda hakkında daha fazla bilgi edinin.

Uygulama

E-Güvenlik Yönetimi

- E-Güvenlik'ten sorumlu atanmış bir personel üyesine sahip olmanız iyi bir şey. Tüm paydaş gruplarından üyelerden oluşan bir e-Güvenlik komitesine sahip olmanın yararlı olup olmayacağını düşünün. Bu kişinin Okul Politikanızın geliştirilmesi ve düzenli olarak gözden geçirilmesi sürecine dahil olmasını sağlayın. Sadece bilgilendirilmekle kalmamalı, aynı zamanda bir olay meydana geldiğinde Olay ele alma formunu da doldurmalıdır. www.esafetylabel.eu/group/teacher/incident-handling

- Teknoloji hızla gelişir. BİT'den sorumlu personelin yeni özelliklerden ve risklerden haberdar olmak için düzenli olarak eğitimlere ve / veya konferanslara gönderilmesi iyi bir uygulamadır. Çevrimiçi dünyadaki en son trendlerden haberdar olmak için Better Internet for Kids portalına göz atın.

Müfredatta e-Güvenlik

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

- Okulunuzda sosyal medyayı kullanırken çocuklara küçük yaşlardan itibaren sorumluluklar ve sonuçlar hakkında eğitim verilmesi çok iyi. Lütfen herhangi bir kaynağı kanıt yükleme aracı aracılığıyla paylaşın, Okulum alanından da erişilebilir.

- Okulunuzdaki tüm yıl gruplarındaki tüm öğrencilere e-Güvenlik hakkında eğitim verilmesi iyi bir uygulamadır. Sürekli değişen ihtiyaçları karşıladığından emin olmak için müfredat hükmünü düzenli olarak gözden geçirmek önemli olmaya devam etmektedir. Bu türden bir müfredat inceleme süreciniz varsa, bunu okul profilinizde yayınlarsanız diğer okullar için faydalı olacaktır. Yüklemek için Okul alanınıza gidin.

- Okulunuzda Siber Zorbalığın müfredatta genç yaştaki öğrencilerle tartışılması iyi bir uygulamadır.

Müfredat dışı etkinlikler

- Müfredat dışı zamanlardan ne tür ek e-Güvenlik desteğinden yararlanacaklarını görmek için öğrencilerden geri bildirim toplayın. Bunların bir kısmını meslektaşlarına ulaştırmaya dahil olabilirler mi? Bunu yapmalarına yardımcı olacak kaynakları bulmak için e-Güvenlik Etiketi portalındaki kaynak bölümünü kontrol edin; Öğrencilerin okul dışında çevrimiçi teknoloji www.esafetylabel.eu/group/community/pupils-use-of-online-technologyoutside-school.

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 bunu kopyalayabilir.

- Diğer okul hizmetlerinin e-Güvenlik konularına dahil olduğunu bilmek iyidir (örn. Danışmanlar, psikologlar, okul hemşiresi). Okul Politikanızın geliştirilmesine ve düzenli olarak gözden geçirilmesine katkıda bulunmaya da davet ediliyorlar mı? Okulunuzda bunun nasıl yönetildiğiyle ilgili bir vaka çalışmasını e-Güvenlik Etiketi proje web sitesindeki okulunuzun profil sayfasında yayınlayın, böylece diğerleri sizin deneyimlerinizden öğrenebilir.

Personel eğitimi

- Tüm personelin e-Güvenlik konularında düzenli eğitim alması öğrencileriniz için gerçek bir fayda sağlayacaktır. Eğitimin orta ve uzun vadeli faydaları hakkında personelden geri bildirim almaya devam edin ve www.esafetylabel.eu/group/community/suggestions-for-onlinetraining-courses adresindeki eğitim kurslarına yönelik önerileri görmek için eSafety Label portalına başvurun.

Gönderdiğiniz Değerlendirme Formu büyük bir soru havuzundan oluşturulmuştur. Ankette belirtilmeyen alanlarda e-Güvenliği iyileştirip iyileştirmediğinizi bilmek de bizim için yararlıdır. Bu tür değişikliklerin kanıtını, e-Güvenlik Portalının Okul alanım bölümündeki Kanıtı yükle yoluyla yükleyebilirsiniz. Unutmayın, Değerlendirme Formunun doldurulması Akreditasyon Sürecinin sadece bir parçasıdır, çünkü kanıtların yüklenmesi, Forum aracılığıyla başkalarıyla görüşmeleriniz ve sağlanan şablonda olayların raporlanması da hesaba katılır.