e-Güvelik Etiketi - Eylem Planı

Bu eylem planı 3 ana başlık hakkında yararlı tavsiye ve yorumlar önermektedir.

ALTYAPI

Teknik Güvenlik:

- Tüm yaş gruplarındaki öğrencilerde eğitici bir yaklaşım ve esneklik inşa etmek güvenli ve sorumlu internet kullanımı için bir anahtardır. Bu sebeple öğrencilerinize karşı iyi ve güvenli bir dijital vatandaş olmaları hakkında nasıl konuşacağınıza dair öğretmenlerinizi bir araya getirin ve bu konuda bir tartışma başlatın.

Öğrenci ve personelin teknolojiye erişimi:

- Okulunuzda bilgisayar erişimin olması bir avantajdır. Diğer dijital cihazların da derslere entegre edilmesi seçeneğini düşünün çünkü öğrencilerin yeni medyayla ilgilenmeleri için en iyi pratiği sağlar.

Verilerin Korunması:

- Okulunuzda farklı şifrelerin kullanıldığı bir sistemin olması bir avantajdır. Şifrelerin kimseyle paylaşılmaması konusunda öğretmen ve öğrencilerinizi uyarın.
- Öğrenme ve yönetim çevrelerinizin birlikte olması bir güvenlik riski oluşturabilir. Öğrencilerin ve personelin özel verilerinin korunması okulun esas rolüdür. e- Güvenlik yöneticisi, personel ve bir uzman ile öğrenme ve yönetim çevrelerinin ayrılması için bir strateji belirlenip uygulanmasını tesviye ederiz.

Yazılım Lisansı

- Okulunuzdaki tüm yazılımların yasal olarak lisanslı olduğundan ve kopyalarının merkezi olarak tutulduğundan/saklandığından emin olun.
- Bilişim sistemlerini destekleyen sorumlu kişi ile yazılımın sistem güvenliğinden taviz vermediğini kontrol etmelisiniz.
- Okulunuzun yazılım tedariki için açık bir politika geliştirmelisiniz.

Bilişim Teknolojileri Yönetimi

- Okulunuzda sadece yönetici ya BT öğretmeni yazılım alımında sorumlu görünmektedir. Öğretmenlerin de yazılım isteğinde bulunabileceği bir sistem düşünmelisiniz.

POLİTİKA

Kabul edilebilir kullanım politikaları (AUP) raporu ve Olay Yönetimi

- Okul politikanızın, öğrencilerin bilerek ya da yanlışlıkla yasadışı ve uygunsuz içerikle karşılaşmaları halinde öğretmenlerin neler yapması gerektiği ile ilgili gerekli bütün bilgileri içerdiğinden emin olun.
- Böyle durumların yaşanması halinde e-Güvenlik Olay Yönetimi formunu isimsiz bir şekilde detayları ve çözümü ile paylaşınız. Böylece diğer sorun yaşayan okullar da faydalanabilir.
- Okulunuzda öğretmenleriniz siber zorbalık durumlarını fark etme ve yönetme becerisine sahip. Öğrenci ve veliler arasında farkındalık yaratmak için yöntemler düşünmelisiniz.
- e-Güvenlik olay yönetimi bölümünde yaşanan zorbalık durumlarından bahsedilmemesi üzücü bir durumdur. Bu forumda paylaşılması halinde tecrübelerden faydalanılabilir.
- Okul Kabul edilebilir kullanım politikalarında (*AUP)* zorbalık karşıtı yönergelerin öğrenci ve personele verildiğinden emin olun.
- Okul dışı e-Güvenlik olaylarının yönetimi hakkında açık bir Okul Politikanızın olması bir avantajdır. Bu durum olayların azalmasını sağlıyor mu? Yaşanan olayların daha da azaltılması için farkındalığı artırmak ve koruyucu önlemler almak adına bir tartışma konusu başlatın.

- Diğer okulların da faydalanması için e-güvenlik olay yönetimi bölümünde yaşanılan durumları ve çözümleri paylaşmayı unutmayın.

Personel Politikası

- Kabul Edilebilir Kullanım Politikanızda (AUP) öğretmenlerin sınıfta cep telefonlarını kullanmalarına ilişkin yönergeleriniz var.
- Diğer eSafety Label okullarına yardımcı olabilecek bir iyi uygulama modeli olduğundan, AUP'nizi okul profilinize yükleyin.

Öğrenci Uygulama/Davranışı

- Okulunuz, öğrenci davranışı için okul çapında olumlu ve olumsuz sonuçlara yönelik bir yaklaşıma sahiptir. Bu iyi bir uygulama, diğer okulların öğrenebilmesi için lütfen eGüvenlik portalının Okulum alanı aracılığıyla politikanızı paylaşın.

Okul Çevrimiçi Görünümü

- Okulda fotoğraf, video çekme ve yayınlama konusundaki bilgi notunu (www.esafetylabel.eu/group/community/taking-and-publishing-photos-and-videos-at-school) kontrol edin.
- Okul Politikanızın bu bölümünü **Okulum Alanı** (My School Area) aracılığıyla profil sayfanıza yükleyin Böylece diğer okulların da sizin iyi uygulamalarınızdan faydalanmasını sağlayın.
- Okulunuzun çevrimiçi bir varlığı olsa da, öğrenciler bunun şekillenmesinde yer almamaktadır. Öğrencilerinizin de sürece dahil olması için yöntemler araştırın. Aynı zamanda bir akran destek ağı oluşturmaya da yardımcı olabilir.
- Okulun sosyal medya sitelerindeki çevrimiçi varlığının içeriğini, uygunsuz yorumların olup olmadığını düzenli bir şekilde kontrol ederek herhangi bir sorun olmadığından emin olun.
- Siteyi/sayfayı güncel tutmak için bir süreç oluşturun ve daha fazla bilgi için sosyal ağlardaki okullar (www.esafetylabel.eu/group/community/schools-on-social-networks) bilgi formunu kontrol edin.
- Profilin ne kadar yararlı olduğu hakkında paydaşlardan geri bildirim alın.

UYGULAMA

e-Güvenliğin Yönetimi

- e-Güvenlik için seçilen sorumlu kişinin veya yönetim kurulu üyesinin düzenli olarak eğitim almasını ve ayrıca personelin e-Güvenlik sorunlarından haberdar olmalarını sağlayın.
- Yönetim kadronuzun okul politikanızın geliştirilmesi ve düzenli olarak gözden geçirilmesi sürecine dahil edin. Okul Politikası hakkındaki bilgi notumuza (www.esafetylabel.eu/group/community/school-policy) bakın.

Müfredatta e-Güvenlik

- Çocuk koruma politikanızda cinsel içerikli mesajlaşmaya özel olarak atıfta bulunmanız sizin için avantaj sağlamaktadır, çünkü bu bir birçok gencin uğraşmak zorunda kaldığı büyüyen bir sorun haline gelmiştir.
- Öğrencilere bu konuda uygun eğitimin verildiğinden emin olun.
- Cinsel içerikli mesajlaşmanın okul genelinde daha geniş çevrimiçi güvenlik eğitimine entegre edilmiş olması sizin için avantaj sağlamaktadır.
- Bu eğitimin etkisini değerlendirebiliyor musunuz ? Öğrencilerin davranışlarını değiştirmelerine yardımcı oluyor mu? Nerden biliyorsunuz?
- e-Güvenliğin okulunuzdaki müfredatın bir parçası olarak öğretilmesi sizin için avantaj sağlamaktadır.
- Tüm personelin eGüvenlik eğitimi aldığından emin olun.

- Siz/personeliniz, eSafety'i Sisteme Yerleştirme hakkında bilgi notunda (www.esafetylabel.eu/group/community/embedding-online-safety-in-curriculum) bazı yararlı fikirler ve kaynaklar bulabilirsiniz.
- Okulunuzda siber zorbalığın müfredatta küçük yaşlardan itibaren öğrencilerle tartışılması iyi bir uygulamadır.

Müfredat dışı faaliyetler

- Akran danışmanlığında öğrencilerin katılımını daha da geliştirmeye çalışın.
- Öğrencilerin düşüncelerini ve anlayışlarını akranlarıyla paylaşmaları için onlara daha fazla fırsat sağlayın.
- Daha fazla fikir ve kaynak almak için eSafety'nin kaynak bölümüne de göz atın.
- Öğrencilerinizin çevrimiçi alışkanlıkları hakkında sahip olduğunuz bilgileri diğer okullarla paylaşmayı düşünün.
- Örneğin, öğrencilerin çevrimiçi alışkanlıklarına ilişkin en son anket bulgularınızı Okulum Alanınız **(My School Area)** aracılığıyla okul profilinize ekleyin.

Destek Kaynakları

- Ebeveynlerden kendilerine sağlanan e-Güvenlik desteğinin türü hakkında geri bildirim isteyin ve faydalanan aile sayısını artırmak için yenilikçi yollar düşünün. Ebeveynler için bilgi sayfasını (www.esafetylabel.eu/group/community/information-for-parents) ziyaret edin.
- E-Güvenlik konularında bilgi sahibi olan ve E-Güvenlik konusunda öğrencilere güven veren bir personelinizin olması sizin için avantaj sağlamaktadır..

Personel Eğitimi

- Gönderdiğiniz Değerlendirme Formu, geniş bir soru havuzundan oluşturulmuştur. Ankette bahsedilemeyen e-Güvenlik alanlarında da kendinizi geliştirip geliştirmediğinizi görmemizi sağlayan kullanışlı bir formdur.
- eGüvenlik Portalı nın Okulum Alanı sekmesine değişim kanıtlarınızı yükleyebilirsiniz.
- Unutmayın ki, Değerlendirme Formunun doldurulması, değerlendirmenin yalnızca bir parçasıdır.
- Akreditasyon Sürecinde, delil yükleme, başkaları ile yaptığınız alışverişler aracılığıyla forum ve sağlanan şablondaki olayları raporlamanız da dikkate alınır.