

eGüvenlik Etiketi - Eylem Planı

Doldurduğunuz Değerlendirme Formunu eSafety Label portalına göndererek,

okulunuzdaki e-Güvenlik durumunu analiz etmeye yönelik önemli bir adım. Tebrikler! Lütfen

eSafety'i daha da geliştirmek için neler yapabileceğinizi görmek için Eylem Planınızı dikkatlice okuyun.

Okul. Eylem Planı, 3 temel alana bölünmüş yararlı tavsiyeler ve yorumlar sunar:

altyapı, politika ve uygulama.

ALTYAPI

TEKNİK GÜVENLİK

- BİT hizmetlerinizin düzenli olarak gözden geçirilmesi, güncellenmesi ve artık kullanılmıyorsa kaldırılması önemlidir.
- Yükleme en son sürümler ve yamalar genellikle hizmetlerinizin gelebileceği güvenlik açıklarını giderir saldırı altında. Bunun BİT koordinatörünün iş tanımının bir parçası olduğundan emin olun.
- Okul sisteminiz bir güvenlik duvarı tarafından korunmaktadır. Güvenlik duvarının sağlanmasının ve yönetiminin düzenli olarak gözden geçirilir ve gerektiğinde güncellenir.
- Her yaşta öğrencide bir eğitim yaklaşımı ve dirençlilik oluşturmak da güvenli ve sorumlu çevrimiçi için anahtardır. bu yüzden tüm öğretmenleri, öğrencileriyle iyi biri olma hakkında nasıl konuşacaklarını tartışmak üzere bir araya getirin.
- güvenli dijital vatandaş, Avrupa'da gerçekleştirilebilecek tartışma örnekleri için bkz. www.europa.eu/youth/EU_en
- Rol yapma ve grup oyunları yoluyla bu konuda sınıf.

ÖĞRENCİ VE PERSONELİN TEKNOLOJİYE ERİŞİMİ

- Mobil cihazları yasaklamanın amaca uygun bir kural olup olmadığını ve okulunuzun buna izin verip vermeyeceğini düşünün.
- Bazı sınıf etkinlikleri için dijital cihazlar kabul Edilebilir Kullanım Politikanızın bir parçası olarak, nasıl yapılacağına ilişkin bir bölüm geliştirebilirsiniz.
- Dijital teknolojiler sınıfta kullanılabilir ve kullanılamaz; adresindeki Cep Telefonlarını Kullanma hakkındaki bilgi formuna bakın.
- Okul (www.esafetylevel.eu/group/community/using-mobile-device-in-schools).
- Tüm personel ve öğrencilerin okulunuzda USB bellek kullanmasına izin verilir. Bu iyi bir uygulamadır ve sizin Kabul Edilebilir Kullanım Politikası, okul sistemlerinde kullanılmadan önce tüm çıkarılabilir ortamların kontrol edilmesini şart koşmalıdır.
- Tüm güvenlik hususlarını kapsadığınızdan emin olmak için www.esafetylevel.eu/group/community/use-of-removabledevices adresindeki Çıkarılabilir cihazların kullanımı hakkındaki bilgi notunu kontrol edin.
- Okulunuzdaki dizüstü bilgisayarlara/tabletlere bir derste kolayca erişilebilmesi harika. Bunları kullanmak en iyisini sağlar

- öğrenciler için yeni medya ile ilgili alıştırmalar. Güvenlik konularının da tartışıldığından emin olun.
- Personel ve öğrenciler okul ağınızda kendi ekipmanlarını kullanabilecekleri için, Kabul Edilebilir Kullanım Politikası, okulun tüm üyeleri tarafından düzenli olarak gözden geçirilir ve gerektiğinde uyarlanır. Olmalı Onları korumak için neyin yürürlükte olduğunu anlamaları için her akademik yılın başında öğrencilerle tartışılır ve mahremiyetleri ve neden. Politikayı teknoloji den çok davranışa dayandırın. Ziyaretçiler ayrıca okumalı ve okulun ağını kullanmadan önce Kabul Edilebilir Kullanım Politikasını imzalayın.

Veri koruması

- Okulunuzdaki sistem tarafından tüm kullanıcılara farklı bir parola atanması iyidir. Tüm okula hatırlat
- üyeler, kendilerine verilen şifreyi hiçbir yere, kesinlikle bilgisayardaki bir çıkartmaya yazmamalıdır! Ayrıca, Kabul Edilebilir Kullanım Politikasının personele ve öğrencilere şifrelerini güvende tutmalarını ve paylaşmamalarını hatırlattığından emin olun onları başkalarıyla Öğrenim ve yönetim ortamlarınızın bir arada olması bir güvenlik riski oluşturabilir.
- güvenliğinin sağlanması personelin ve öğrencilerin özel verileri okulun temel bir rolüdür.
- Atanan eSafety'nin yönetici/BİT koordinatörü, personel ve bir teknik uzmanla birlikte, aşağıdakiler için bir strateji tanımlar ve uygular: öğrenme ve yönetim ortamlarını ayırmak veya eşdeğer en yüksek güvenlik seviyesini sağlamak onların arasında. Şuradaki okullarda hassas verilerin korunması hakkındaki bilgi notunu okuyun:
- www.esafetylevel.eu/group/community/protecting-responsive-data-in-schools.

YAZILIM LİSANSLAMA BT YÖNETİMİ

BT ağından sorumlu kişinin hangi yazılımın açık olduğu konusunda tam olarak bilgilendirildiğinden emin olunması iyi bir uygulamadır.

Okula ait donanımdır ve bu, Okul Politikasında ve Kabul Edilebilir Kullanım Politikasında açıkça belirtilmelidir.

Ağdan sorumlu kişinin, lisans gerekliliklerine uygunluğu garanti edebilmesi gerekir. ve bu yeni yazılım ağ çalışmasına müdahale etmez.

POLİTİKA

Kabul Edilebilir Kullanım Politikası (AUP)

- Okulunuzda öğretmenlerin ve öğrencilerin ilgili okul politikalarını imzalamaları iyi bir uygulamadır.
- Öğrencilerle önceden tartışıldı. Bunları ve uygunsuzlukların nerede olduğunu tartışmak için düzenli toplantılar yapmayı düşünün ele alınır.

- eGüvenliğin birçok okul politikasının ayrılmaz bir parçası olması harika. Tüm personel ne zaman buna atıfta bulunuyor öğretim yoluyla uygun mu? İyi uygulama örnekleri arayın ve bunları personel ve öğrencilerle paylaşın.
- Bu iyi uygulamayı vurgulamak için kısa bir vaka çalışması hazırlayın ve eSafety Label portalındaki profilinize yükleyin.
- Diğer okullar için ilham kaynağı olarak Benim okulum alanınız aracılığıyla

Raporlama ve Olay Yönetimi

- Zorbalık olaylarına uygulanan detayların ve çözüm yollarının hem çalışanlarla hem de sosyal medya üzerinden paylaşılmaması üzücü.
- eSafety Label olay işleme formu. Ancak bu şekilde deneyimle ve başarılı olarak öğrenebilirsiniz.başkalarının olay işleme uygulamaları. Zorbalığa karşı yönergelerin öğrencilere verildiğinden de emin olmalısınız.
- Kabul Edilebilir Kullanım Politikanızdaki personel. Yeni personel de dahil olmak üzere tüm personelin, aşağıdaki durumlarda ne yapılacağına ilişkin yönergelerin farkında olduğundan emin olun: bir okul makinesinde uygunsuz veya yasa dışı materyal keşfedildiğinde. Politikanın titizlikle uygulandığından da emin olun
- Zorunlu Okulun kıdemli liderlik ekibinin bir üyesi bunu izlemelidir.
- Okul Politikanızın, öğretmenler için öğrencilerle iletişim kurarken sorunları ele almayla ilgili tüm gerekli bilgileri içerdiğini kontrol edin.
- belirlenen kılavuza giderek yasa dışı veya rahatsız edici materyallere çevrimiçi olarak bilerek veya yanlışlıkla erişin.
- Teachingtoday.de/en web sitesi (tinyurl.com/9j86v84). Okulunuzda bu tür olaylar meydana gelirse,
- eSafety Etiketi Olay işleme formunu (www.esafetylabel.eu/group/teacher/incidenthandling) anonim olarak doldurun, böylece diğer okullar sizin deneyiminizden faydalanabilir.

Personel politikası

- Okul politikasının potansiyel olarak güvenli olmayan cihazlarla ilgili riskler hakkında bilgi içermesi iyi bir uygulamadır.
- akıllı telefonlar gibi ve bu referans ona yapılır. Okul politikanızı yükleme yoluyla paylaşmayı düşünün
- Okulum alanından da erişilebilen kanıt aracı.

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 olaylar. Etkili, sorumlu iletişim hakkında bilgi edinmek de eğitimin bir parçası olmalıdır.

- Her genç için gerekli bir yeterlilik olduğu için okul müfredatı. Bunu bir personel toplantısında tartışın uygulamak istediğiniz standartları tanımlamak için.
- Müfredat dışı olsun, eGüvenliği tartışırken öğrencilerin okul etkinliklerini şekillendirme olanağına sahip olması iyidir.
- Günlük yaşamlarında olup bitenlere bağlı olarak müfredat programları. Bu şekilde daha meşgul olacaklar ve aynı zamanda öğretmenin gerçek yaşam sorunlarını tanımasını sağlar.

Çevrimiçi okul varlığı

- Okulunuzun çevrimiçi itibarını izlemek için özel bir kişiye sahipsiniz ve bu iyi bir uygulamadır.
- Her zaman ol düzenli bir aramayla hemen görünmeyebilecek yeni sitelerin farkında.
- Güncel tutun özellikle okullar ve öğrenciler için zarar verebileceklerinden ve bunları düzenli aralıklarla
- personel olumsuz bir bakış açısı sunarsa.
- Okulda fotoğraf ve video çekme ve yayınlama konusundaki bilgi notunu kontrol edin
- (www.esafetylabel.eu/group/community/taking-and-publishing-photos-and-videos-at-school)
- Okul Politikanızın tüm alanları kapsar, ardından Okul Politikanızın bu bölümünü My aracılığıyla profil sayfanıza yükleyin.
- Diğer okulların sizin iyi uygulamalarınızdan öğrenebilmesi için okul alanı.

PRATİK

eGüvenlik yönetimi

- Okulunuzdaki tüm personelin e-Güvenlikten sorumlu olması iyidir. Ancak, bir kişinin atanması iyi bir uygulamadır.
- Gerekli odağı sağlamak için e-Güvenlik konularında genel sorumluluğa kim sahip olacaktır. İdeal olarak bu olmalıdır.
- kıdemli liderlik ekibinden biri. Bu kişinin geliştirme sürecine dahil olduğundan emin olun ve düzenli olarak
- Okul Politikanızın gözden geçirilmesi. Yalnızca bilgilendirilmemeli, aynı zamanda Olay yönetimini de doldurmalıdır.
- www.esafetylabel.eu/group/teacher/incident-handling adresinde bir olay meydana geldiğinde oluşturulur.
- Teknoloji hızla gelişir. BİT'ten sorumlu personelin düzenli olarak şuraya gönderilmesi iyi bir uygulamadır:
- yeni özelliklerin ve risklerin farkında olmak için eğitimler ve/veya konferanslar. Çocuklar İçin Daha İyi İnternet portalına göz atın çevrimiçi dünyadaki en son trendlerden haberdar olmak için.
- Okulunuzda, öğretmenler kendi öğrencilerinin çevrimiçi aktivitelerinden sorumludur. Birçok ağ güvenliği vardır ve güvenliğinizi sağlamak için yapılması gereken kullanıcı gizliliği, denetim ve prosedürel araç kontrolleri ve dengeleri öğrenciler ve okul ağları ve bunlar Okul Politikanızda belirtilmelidir. Adresindeki bilgi sayfamıza bakın

- www.esafetylevel.eu/group/community/school-policy adresindeki Okul Politikası.
- Bunun gerektiđi kadar verimli ve sıklıkla gerekleřmesini sađlamak iin, okulunuzun M¼d¼r¼ne řunları tavsiye ediyoruz:
- okuldaki e-G¼venlik y¼netimiyle ilgilenmesi iin bir bireysel personel ¼yesi atar. bu kiři olacak
- Okul Politikanızda yer alan t¼m hususların bařkalarıyla tartiřılmasını ve ele alınmasını sađlamaktan sorumludur. ¼đretmenler ve sınıftaki ¼đrencilerle birlikte.
- Her personel ¼yesinin, ¼đrencinin ve velinin kendi evrimii haklarının ve sorumluluklarının farkında olmasını sađlamak iin, bkz.
- Kabul Edilebilir Kullanım Politikası hakkında bilgi formu (www.esafetylevel.eu/group/community/acceptable-use-policy-aup-).

M¼fredatta e-G¼venlik

- Okulunuzda siber zorbalıđın m¼fredatta k¼¼k yařlardan itibaren ¼đrencilerle tartiřılması iyi bir uygulamadır.
- e-G¼venliđin okulunuzdaki m¼fredatın bir parası olarak ¼đretilmesi iyidir. T¼m personelin eSafety sađladığından emin olun.
- M¼fredat boyunca ve sadece BİT veya Kiřisel Sosyal ve Sađlık yoluyla deđil, uygun olduđunda eđitim dersler. Siz/personeliniz, eSafety'i Sisteme Yerleřtirme bilgi notunda bazı yararlı fikirler ve kaynaklar bulabilirsiniz.
- www.esafetylevel.eu/group/community/embedding-online-safety-in-curriculum adresindeki m¼fredat.
- Cinsel ierikli mesajlařma, birok genci etkileyen bir konudur. Olası sonuları ve riskleri onlarla paylařmak, konu etrafında biraz tartiřma firsatı kadar ¼nemlidir. Cinsel ierikli mesajlařma, geniř ve dengeli e-G¼venlik m¼fredatı.
- Bu konuların e-G¼venlik m¼fredatına dahil edilmiř olması g¼zel. d¼zenli olarak g¼zden geirmek iyi bir fikirdir.
- Yeni ve ortaya ıkan sorunların ortadan kaldırılmasını sađlamak iin e-G¼venlik eđitiminizin kapsadıđı sorunlar kapalı.

M¼fredat dıřı etkinlikler

- ¼đrencilere okul dıřında karřılařtıkları evrimii g¼venlik sorunlarıyla bařa ıkılmaları iin destek sunmayı d¼ř¼n¼n ve not alın bunları eSafety Label topluluđundaki diđer okullarla paylařmak iin. yardımcı olmak iin bir "ameliyat" sađlamak yararlı olabilir.
- eG¼venlik Etiketini portalı bunun iin yararlı olacak kaynaklar sađlar;
- ¼đrencilerin evrimii teknolojiyi okul dıřında kullanımına iliřkin bilgi notuna řu adresten g¼z atın:
- www.esafetylevel.eu/group/community/pupils-use-of-online-technology-outside-school.
- Daha G¼venli İnternet G¼n¼'n¼ t¼m okul topluluđunu evrimii g¼venlik konusuna dahil edecek bir mekanizma olarak kullanın. Bu www.saferinternetday.org adresinde bulunan bilgi ve kaynaklar, akranları teřvik etmek iin ideal bir firsat sunar.

Destek kaynakları Personel eğitimi

- Okulunuz, her öğretmenin siber zorbalık konusunda eğitildiğinden emin olur. Lütfen kullanılan kaynakları paylaşın.

Gönderdiğiniz Değerlendirme Formu, geniş bir soru havuzundan oluşturulmuştur. Ayrıca kullanışlıdır ankette belirtilmeyen alanlarda eGüvenliği geliştirip geliştirmediğinizi bilmemiz için. Yapabilirsiniz

Bu tür değişikliklerin kanıtlarını Okulum alanım bölümündeki Kanıtları yükle aracılığıyla yükleyin.

eGüvenlik Portalı. Unutmayın, Değerlendirme Formunun doldurulması, değerlendirmenin yalnızca bir parçasıdır.

Akreditasyon Süreci, çünkü delil yükleme, başkaları ile yaptığınız alışverişler aracılığıyla

Forum ve sağlanan şablondaki olayları raporlamanız da dikkate alınır.