**E SAFETY LABEL BRONZ MADALYA EYLEM PLANI**

**Eylem Planı, 3 temel alana bölünmüş faydalı tavsiyeler ve yorumlar sunar: altyapı, politika ve uygulama.**

**Altyapı**

**Teknik güvenlik**

Tüm okul cihazlarınızın virüs korumalı olması çok iyi. Hem okul politikanıza hem de Kabul Edilebilir Kullanım Politikanıza virüs koruması ile ilgili bir paragraf eklediğinizden ve personelin ve öğrencilerin okul yönergelerini titizlikle uyguladığından emin olun. Daha fazla bilgiye ihtiyacınız varsa,

www.esafetylabel.eu/group/community/protecting-your-devices-against-malware

adresindeki Cihazlarınızı kötü amaçlı yazılımlara karşı koruma konulu bilgi belgesine bakın.

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

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**

Okulunuzda bilgisayar laboratuarlarının kolayca rezerve edilebilmesi iyidir. Diğer dijital cihazları derslere entegre etme seçeneğini düşünün, çünkü bunları kullanmak, yeni medya ile uğraşırken öğrenciler için en iyi uygulama sağlar. Güvenlik konularının da tartışıldığından emin olun.

Okul içinde farklı amaçlar için farklı WiFi ağları sağlamanız gerekir, örn. personel / çekirdek iş için güvenli bir ağ, ziyaretçiler için bir misafir ağı ve gündelik kullanım.

Personel ve öğrencilerin okul ağında kendi ekipmanlarını kullanmaları, bir Kabul Edilebilir Kullanım Politikasında ele alınmalıdır, böylece kullanıcılar hangi ağları ve neden kullanmaları gerektiği konusunda nettir. Kabul Edilebilir Kullanım Politikanız, okul ağında hangi faaliyetlere izin verildiği ve nelere izin verilmediğine dair net bir kılavuz içermelidir.

**Veri koruması**

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. Bir şifreleme sistemi aracılığıyla okul profilinize hassas verileri korumayla ilgili bazı yönergeleri yükleyin. Böylece diğer okulların deneyimlerinizden yararlanabilir.

**Yazılım lisanslama**

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.

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.

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

**BT 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.

**Politika**

**Kabul Edilebilir Kullanım Politikası (AUP)**

ESafety'nin çeşitli okul politikalarının ayrılmaz bir parçası olması mükemmeldir. Tüm personel, uygun olduğunda öğretim yoluyla buna referans veriyor mu? İyi uygulama örneklerini araştırın ve bunları personel ve öğrencilerle paylaşın. Bu iyi uygulamayı vurgulamak için kısa bir vaka çalışması hazırlayın ve bunu diğer okullar için ilham kaynağı olarak Okul alanınız aracılığıyla e-Güvenlik Etiketi portalındakiprofilinize yükleyin.

**Raporlama ve Olay Yönetimi**

Okul dışı e-Güvenlik olaylarının üstesinden gelmek için net bir Okul Politikasına sahip olmanız iyidir; Bunların sayısı azalıyor mu? Sorunların sayısını daha da azaltmak için başka hangi önleyici tedbirlerin veya farkındalık artırma faaliyetlerinin kullanılabileceği konusunda toplulukta bir tartışma dizisi başlatın. Okulların birbirlerinin stratejilerini paylaşmalarına ve onlardan öğrenmelerine olanak sağladığından, Olayları ele alma formunda (www.esafetylabel.eu/group/teacher/incident-handling) olayları isimsiz olarak belgelemeyi unutmayın.

Yeni personel de dahil olmak üzere tüm personelin, bir okul makinesinde uygunsuz veya yasadışı materyal bulunursa ne yapılacağına ilişkin yönergelerden haberdar olduğundan emin olun. 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.

**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.

**Öğrenci alıştırması / davranışı**

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 ( My schoolarea ) üzerinden okul profilinize yükleyin.

**Çevrimiçi okul varlığı**

Okul Politikanızın tüm alanları kapsadığını görmek için okulda fotoğraf ve video çekme ve yayınlama hakkındaki bilgi formunu kontrol edin (www.esafetylabel.eu/group/community/taking-and-publishing-photos-and-videos-at-school), daha sonra Okul Politikanızın bu bölümünü, diğer okulların sizin iyi uygulamalarınızdan öğrenebilmesi için Okul alanınız üzerinden profil sayfanıza yükleyin.

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.

Uygunsuz yorum bulunmadığından emin olmak için okulun sosyal medya sitelerindeki çevrimiçi varlığının içeriğini düzenli olarak kontrol edin. Siteyi / sayfayı güncel tutmak için bir süreç oluşturun ve bundan emin olmak için daha fazla bilgi için sosyal ağlardaki Okullar (www.esafetylabel.eu/group/community/schools-on-social-networks) bilgi formunu kontrol edin.

iyiuygulama yönergeleri takip edilmiştir. Paydaşlardan profilin ne kadar yararlı olduğu hakkında geri bildirim alın.

**Uygulama**

**E-Güvenlik Yönetimi**

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.

E-Güvenlik için atanan guvernör veya kurul üyesinin düzenli eğitim alma ve ayrıca meslektaşların e-Güvenlik konularından haberdar olmalarını sağlama fırsatına sahip olduğundan emin olun. Okul Politikanızın geliştirilmesi ve düzenli olarak gözden geçirilmesi sürecine yönetim organınızı dahil edin. Okul Politikası hakkındaki bilgi notumuza bakın: www.esafetylabel.eu/group/community/school-policy

Gerekli tüm ağ güvenliğini ve kullanıcı gizliliğini sağlamak için net bir sorumluluk tanımlamasına ek olarak kontroller uygulandığında, okulların da düzenli aralıklarla denetim ve prosedür kontrollerine sahip olması önemlidir. Bu olmadan, bir okul kendini savunmasız bırakacaktır. Okul Politikası ile ilgili bilgi formumuzuwww.esafetylabel.eu/group/community/school-policy

adresinde bulabilirsiniz.

E-Güvenlik konusunda her zaman okulunuzda olduğu gibi genel bir lider olması gerekmesine rağmen, okuldaki herkesin günlük mesleki görevlerinde kullanılan hassas bilgilerin güvenliğini sağlamak için ortak bir sorumluluğu vardır. Doğrudan veri işlemeye dahil olmayan personel bile riskler ve tehditler ve sorunların nasıl en aza indirileceği konusunda bilgilendirilmelidir. Herkesin olabildiğince en iyi ve en güvenli dijital vatandaş olmalarını sağlamak için üzerlerine düşeni yaptığından emin olmak için Kabul Edilebilir Kullanım Politikası (www.esafetylabel.eu/group/community/acceptable-use-policy-aup-) bilgi sayfamızı kullanın.

**Müfredatta e-Güvenlik**

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

Okulunuzda sosyal medyayı kullanırken çocuklara küçük yaşlardan itibaren sorumluluklar ve sonuçlar hakkında eğitim verilmesi çok iyi. Lütfen kaynakları, okulum alanından da erişilebilen yükleme kanıtı aracı aracılığıyla paylaşın.

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.

**Müfredat dışı etkinlikler**

E-Güvenlik Etiketi 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.

Ulusal Güvenli İnternet Merkezinizdeki çevrimiçi e-Güvenlik kaynaklarını sık sık kullandığınızı bilmekte fayda var. Bu kaynakları okulunuzda yararlı buldunuz mu? Lütfen bunların kullanımı ve değeri ile ilgili görüşlerinizi **info-insafe@eun.org** adresine gönderin.

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

**Destek kaynakları**

Tüm personelin e-Güvenlik konusunda bazı sorumlulukları olmalıdır. Okul danışmanları, hemşireler vb. Bu konularda tavsiye ve rehberlik sağlamak için iyi bir konuma sahiptir ve Okul Politikanızın geliştirilmesine ve düzenli olarak gözden geçirilmesine katkıda bulunmaya davet edilmelidir. Bilgi ve becerilerinden maksimum düzeyde yararlanın ve onlara eğitim vermenin uygun olup olmadığını değerlendirin.

**Personel eğitimi**

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 bölümünden Kanıt yükle yoluyla yükleyebilirsiniz. Unutmayın, Değerlendirme Formunun doldurulması Akreditasyon Sürecinin yalnızca bir parçasıdır, çünkü kanıtların yüklenmesi, Forum aracılığıyla başkalarıyla görüşmeleriniz ve sağlanan şablonda olayların raporlanması da hesaba katılır.