eSafety Etiketleri

eSafety Etiketi, 2012 yılında başlatılan bir Avrupa Okul Ağı girişimidir. Okullar için Avrupa çapında bir akreditasyon ve destek hizmeti olan eSafety Label, eğitim ve öğrenim deneyiminin bir parçası olarak çevrimiçi teknolojiye güvenli erişim için güvenli ve zenginleştirici bir ortam sağlamayı hedeflemektedir.
Öğretmenler, okul müdürleri ve bilişim koordinatörleri için önemli bir politika oluşturma merkezi olan eSafety Label, okulların kendi çevrim içi güvenliğini değerlendirmeleri, iyileştirmeleri, güçlendirmeleri için harekete geçmelerini sağlamaktadır. Okulların kendi çevrim içi güvenlik altyapılarını, politikalarını ve uygulamalarını ulusal ve uluslararası standartlara göre gözden geçirmek eSafety Label sayesinde mümkündür.

Okulunuzun çevrimiçi güvenlik seviyesine ve değerlendirme sürecinde değerlendirilen diğer faktörlere bağlı olarak, aşağıdaki etiketlerden birini alabilirsiniz.

Demir - temel çevrimiçi güvenlik seviyesi
Bronz - çevrimiçi güvenlik konusunda asgari farkındalık
Gümüş - çevrimiçi güvenliğe daha gelişmiş bir yaklaşım
Altın - çevrimiçi güvenliğin tüm alanlarında ve çevrimiçi güvenliğin eğitiminde üstün uygulama

Etiket süreci temelde 3 adımdır.

1. Hazırlık,

2. İletişim kurma, katılım sağlama, katkıda bulunma,

3. Değerlendirme Formunu doldurmadır.

Güvenlik etiketi basamakları şu şekilde özetlenebilir:

1. Öncelikle eSafety Label portalına kayıt olunmalıdır. Bu eğitim modülü hazırlandığı tarih itibari ile portal da Türkçe dil seçeneği bulunmamaktadır. Bu noktada okulda bulunan dil öğretmenlerinden yardım istenebilir.
2. e-Güvenlik etiketi ile ilgili okuldaki öğretmenler, okul yöneticileri fikir alış verişi yapmak üzere mutlaka bir araya gelmelidir. Beyin fırtınası ile okulun e-Güvenlik alanında ki risk haritasının oluşturulması tavsiye edilir.
3. eSafety Label portalında bulunan bilgilendirme tabloları, dokümanlar incelenmelidir. Portalı tüm yönleri ile anlamak başvuru aşama sürecini hızlandırır.

4. Anket soruları cevaplandırılmalıdır. Genel olarak her ay portal da yapılan anket çalışmasında ki soruların cevaplandırılması portala aktif katılım açısından önem taşımaktadır.
5. Okul öğretmen ve yöneticileri okulun e-Güvenlik çalışmaları hakkında veri ve doküman hazırlamaya başlamalıdır. Bu belgeler risk haritaları, öğretmenler kurul kararları, SWOT analizi, okulda konu hakkında yapılan sosyal çalışmalar, e-Güvenlik ile ilgili bilgilendirme toplantıları raporları ve resimleri gibi kaynaklar olabilir.
6. Okulun e-Güvenlik alanında yaşadığı sorunlar belge üzerine işlenmeye, raporlaştırılmaya başlanmalıdır. Bu okulun güçlü ve zayıf yönlerini görebilmesi için önem taşır.
7. Portalın forum bölümüne katılım sağlanmalıdır. Forum bölümüm eğitimcilerin birbirleri ile etkileşim içinde oldukları, bilgi ve deneyimlerini paylaştıkları bölümdür. Bu bölüme okulunuzda yapılan iyi örnekleri lütfen yüklemeyiniz! Sadece etkileşim için kullanınız.
8. Blog sayfasına katılım sağlanmalıdır. Blog sayfasında güncel olarak paylaşılan duyurular takip edilmeli ve istenilirse duyurulara / haberlere yorum yapılmalıdır.
9. Değerlendirme formu aşamasına gelebilmek için portal da gerekli bölümler doldurulmalıdır. Okulunuzun kaydı tamamlandıktan sonra değerlendirme formu aşamasına gelinecektir.
10. Ön kaynaklar gönderilmelidir. Burada okulunuzda yapılan iyi örnek uygulamaları "Our resources" bölümüne, okulda raporlaştırılan sorunlar "Our cases" bölümüne eklenmelidir.
11. Bu aşamalar bittikten sonra e-Güvenlik etiketi ile ilgili okuldaki öğretmenler, okul yöneticileri fikir alış verişi yapmak üzere mutlaka bir araya gelmelidir. Beyin fırtınası ile okulun e-Güvenlik alanında ki risk haritasının oluşturulması tavsiye edilir.
12. e-Güvenlik ile ilgili okulda yaşanan sorunlar "Our cases" bölümünden gönderilebilir.
13. Tüm bu aşamaları tamamladıktan sonra değerlendirme formunun doldurulması aşamasına geçilmelidir. Değerlendirme formunda ki sorular okulun e-Güvenlik alanında yaptığı veya farkında olması gereken detaylı sorular içerir.
14. Değerlendirme formu sisteme teslim edilir. Değerlendirme formu son aşamada portala yüklenir ve sonuç beklenir.
15. "Etiket değerlendirme süreci, değerlendirme formunun puanına, kaynak teslimine ve topluluğa aktif katılıma bağlıdır."
16. Demir / Etiket yok: 22 puandan az puan alırsanız, başvurunuz Demir olarak tanımlanır. Okuldaki e-Güvenlik alanında yapmanız gereken çalışmaları kişiselleştirilmiş eylem planınıza dahil ederek size sunulan öneriler üzerinde çalışmaya başlayın. E-tabloları tekrar okuyun, kaynakları ve olay vakalarını eSafety Label portalında keşfedin ve 3 ay sonra tekrar eSafety Label başvurusu yapmak için tekrar deneyin.

17. Bronz Etiket: Değerlendirme formunuz, üç kategorinin her biri en az beş puan olmak üzere en az 22 puan alırsa, okulunuz Bronz etiket kazanacaktır. Bu, okulunuzda e-Güvenlik alanında güçlü yönlerin olduğunu ancak daha da geliştirilmesi gereken yönlerin olduğu anlamına gelir. Bronz etiket okulunuzun ayrıca çevrimiçi güvenliğe bağlılık gösterdiği anlamına da gelmektedir. Eylem Planında önerilen değişiklikleri uyguladıktan, topluma yeterince katkıda bulunduktan ve 12 ay Bronz Etiket almaya hak kazandıktan sonra değerlendirme formunu tekrar gönderebilirsiniz.

18. Gümüş Etiket: Gümüş Etiket alabilmek için değerlendirme formunuzun en az 44 puan alması gerekir. Değerlendirme Formundaki cevaplarınıza, portalda ki etkinliğinize, kaynaklarınıza ve olaylarınıza bağlı olarak, ulusal eSafety Label Koordinatörü okulunuzun çevrimiçi güvenlik politikasının, uygulamasının ve altyapısının bir Gümüş Etiketi hak edip etmediğine karar verecektir.

19. Altın Etiket: Değerlendirme formunda en az 55 puan alan okullar içindir. Bu etiket için Topluluk'taki kaynaklar, olay vakaları ve etkinlikleri, çevrimiçi güvenliğin tüm alanlarında yoğun çalışılmış uygulamalar sergilenmeli ve çevrimiçi güvenlik eğitimi okul müfredatına dahil edilmelidir. Altın eSafety Etiketi verilen bir okul aktif olarak ebeveynleri destekleyecek ve ayrıca diğer okullardaki meslektaşları için çarpan etkisi ile onlara da yardım sağlayacaktır.

20. İlk aşama sisteme kayıt olmaksızın tüm ziyaretçilere açık olan sekmeler ve bölümler, diğeri ise sisteme kayıt olduktan açılan sekmeler ve bölümlerdir.
21. 1. Aşama: Tüm ziyaretçilere açık bölümler: Ana sayfa üzerinde bulunan sekmelere sayfayı ziyaret eden herkesin ulaşabileceği bölümlerdir. Öncelikle dil seçeneği bölümünden istenilen dil seçilebilir. (Şu an portala Türkçe dil desteği gelmemiştir.)

22. About:"Hakkında" sekmesinde eSafety Label'ın, güvenli ve zenginleştirici bir ortam sağlamayı hedefleyen, öğretme ve öğrenme deneyiminin bir parçası olarak çevrimiçi teknolojiye güvenli erişim için okullar için Avrupa çapında bir akreditasyon ve destek hizmeti olduğundan bahsedilmektedir.

23. eSafety Etiketinin nasıl ortaya çıktığı, uygulanan pilot programlar, araştırma programları, araştırma raporları, kurucu paydaşlar, eSafety şampiyonları ön tanıtımı yine bu açılan sayfa da bulunmaktadır.

24. eSafety Label etiketini geliştirme üzerine yapılan araştırma raporunu incelemeniz tavsiye edilir. Rapora buradan ulaşabilirsiniz.

25. Online safety:"Çevrim içi güvenlik" sekmesinde eSafety Etiketi ile okullara, öğrencilere, ebeveynlere ve personellere çevrimiçi güvenliğin tüm yönlerini ele almalarında yardımcı olmayı amaçlandığından bahsedilmektedir. eSafety Label akreditasyon süreci sayesinde, sisteme kayıtlı olan okulların güçlü ve zayıf yönlerinin belirlendiği ve daha fazla gelişme gerektiren çevrimiçi güvenlik yönlerinin okul eylem planları ile sunulduğu anlatılmaktadır.

26. Alt yapı bölümünde internetin çok çeşitli avantajlar ve fırsatlar sunduğu, ancak içinde risklerinde bulunduğu, olumlu içeriğin yanı sıra okulların çocukları ve gençleri korumaları gereken daha zorlu ve sorunlu alanları olduğundan söz edilmektedir. Filtreleme ve izlemenin okulların uygulayabileceği iki yöntem olduğu ancak bunun kısmi bir çözüm olduğu ifade edilmektedir. Okul ağı güvenli ve korumalı mı, akredite bir internet servis sağlayıcısı kullanıyor musunuz, bir filtreleme / izleme ürünü kullanıyor musunuz? gibi sorular da ele alınmaktadır.
27. Politikalar bölümünde okul politikalarının düzenli olarak gözden geçirilmesi gerektiğinin farkına varılmasının önemli olduğu, özellikle çevrimiçi güvenliği ele alırken tüm paydaşların (öğrenciler, personel ve ebeveynler) güvenli bir ortam yaratma ve sürdürmede okul politikalarının oluşturulmasında ve güncellenmesinde yer almaları gerektiğinden söz edilmektedir. Okulun bir dizi sağlam politika ve uygulaması var mı, kabul edilebilir bir kullanım politikanız var mı, herkes bunun farkında mı; zorbalıkla mücadele politikanız, siber zorbalıkla ilgili referanslar içeriyor mu, güvenlik politikası ihlal edildiği zaman etkili yaptırımlar var mı, okulunuzda bir e-güvenlik koordinatörü atadınız mı? gibi sorular da ele alınmaktadır.
28. Uygulama bölümünde dünyadaki en iyi filtreleme yöntemlerinin bile, çocukları ve gençleri çevrimiçi olduklarında korumak için yeterli olmadığından, bir şeyler ters gittiğinde öğrenciler ne yapacaklarını biliyor mu, sadece bir öğretmene veya ebeveynlere değil, aynı zamanda kullandıkları sitenin sahibine de bir şeyi nasıl bildireceklerinin farkındalar mı? gibi sorular ele alınmaktadır.

29. eSafety Label:

30. "eSafety Etiketi" bölümünde, eSafety Etiketinin 2012'de başlatılan bir Avrupa Okul Ağı girişimi olduğu, amacının Avrupa okullarına ve genişletilmiş okul ekosistemine akreditasyon ve destek sağlamak olduğundan bahsedilmektedir.

31. Avrupa çapında bir akreditasyon ve destek servisi olan eSafety label sisteminin öğretmenler, okul müdürleri, BİT koordinatörleri ve okul personeli için önemli bir araç olduğu, eSafety Topluluğunun katılımcılarına etkileşime girebilmeleri, en iyi uygulamaları paylaşmaları, tavsiye almaları ve zor vakaları nasıl çözdüklerine dair paylaşım alanı sunan ideal bir araç olduğu anlatılmaktadır.

32. Okulunuzun çevrimiçi güvenlik seviyesine ve değerlendirme sürecinde değerlendirilen diğer faktörlere bağlı olarak, aşağıdaki etiketlerden birini alabileceğiniz ifade edilmektedir. Bunlar:
    Demir: Temel çevrimiçi güvenlik seviyesi (Etiket tanımlanmaz)
    Bronz: Çevrimiçi güvenlik konusunda asgari farkındalık
    Gümüş: Çevrimiçi güvenliğe daha gelişmiş bir yaklaşım
    Altın: Çevrimiçi güvenliğin tüm alanlarında ve çevrimiçi güvenliğin eğitiminde üstün uygulama

33. News:"Haberler" sekmesinde e-Güvenlik ile güncel haberler, eSafety Label portalına eklenen yeni modüller ve dosyalar, eSafety Label ile ilgili düzenlenen toplantılar gibi birçok habere bu sayfa üzerinden ulaşabilirsiniz.

34. Partners:"Destekçiler" sekmesinde eSafety etiketinin, birçok lider şirketin (Kaspersky Lab, Liberty Global, Microsoft, Telefonica) ve Avrupa Eğitim Bakanlıklarının (Belçika-Flanders, İtalya ve Portekiz) destek sağlamak için Avrupa Okul Ağı ile güçlerini birleştirmesi nedeniyle ortaya çıkan bir Avrupa Okul Ağı girişimi olduğundan söz edilmektedir. Bu sayfada çevrimiçi güvenlik konularında okulların akreditasyonunun birçok kuruluş tarafından desteklendiği bilgilerine ve ilgili endüstri ortakların ve ulusal ortakların tanıtımına yer verilmiştir.

35. Ayrıca sayfada ortak olmak isteyen kuruluşlar için iletişim bağlantısı verilmiştir.

36. eSafety Champions:"e-Güvenlik şampiyonları" sekmesinde ücretsiz çevrimiçi kurslara katılıp bilgi ve tecrübenizi arttırabileceğinizin anlatıldığı sayfada, bu çevrimiçi kursların eSafety politikalarının oluşturulmasında, eSafety risklerini belirlenmesinde, okulların öğrencilere yönelik yaklaşımlarının oluşmasında fayda sağlayacağı ifade edilmektedir.
37. e-Güvenlik şampiyonları çevrimiçi kursunun (MOOC) öğrenme hedeflerinin öncelikle kişiselleştirilmiş eSafety stratejinizi oluşturmak olduğu anlatılmaktadır. Sonrasında okul bağlamında uygun eSafety politikalarının önemini düşünmenin; okulunuzun ve öğrencilerinizin karşılaşabileceği eSafety risklerini ve zorluklarını belirlemenin; öğretmenler, ebeveynler, okul yönetim ekibi, BİT uzmanları vb. katılımı ile okulunuzun ihtiyaçlarına uygun bir eSafety stratejisi geliştirilmesinin önemi vurgulanmaktadır.

38. Community:"Topluluk" sekmesinde hesabınızı ayarları bölümü bulunmaktadır. Akreditasyon işleminize profilinizi ve okulunuzun veya kuruluşunuzun profilini tamamlayarak başlamanız gerektiği anlatılmaktadır. Diğer üyelerin kim olduğunu ve nereden geldiğini bilmelerine yardım etmenin topluluktaki deneyimini geliştireceği vurgulanmaktadır.
39. Topluluğun tüm araçlarını keşfetmenizi, okulunuzun çevrimiçi güvenliğini artırmak için neler yapabileceğinizi ve belgelendirmek için bir eSafety Etiketini nasıl alabileceğiniz bilgilerinin bulunduğu sayfadır. Kullanıcı profili ve okul hesabına bu sayfadan ulaşılmaktadır.

40. Prepare:"Hazırlık" sekmesi öz değerlendirme süreci hazırlıklarının yapıldığı bölümdür. Uluslararası öğretmenler topluluğuna, yöneticilere ve çevrimiçi güvenlik uzmanlarının

olduğu eSafety portalına katılarak okulunuzun çevrimiçi güvenliğini artırma yolunda ilk adımı atmış olduğunuz anlatılmaktadır.

41. Kapasite geliştirmenin eSafety Etiketini edinmede ilk adım olduğu, e-Güvenlik sürecinin devamlı olduğu, okulların akranlar ve uzmanlarla bilgi alışverişinde bulunmaları gerektiği, eğitimcilerin kişisel deneyimlerinden örnekler sağladıkları katılım aşamasının önemli olduğu vurgulanmaktadır. Bütün bunların ise, eSafety etiketi iletişim araçlarıyla (Bloglar, Forumlar, Anketler, Elçilerin Bölümü) sağlandığı sayfada anlatılmaktadır.

42. Son olarak, kapasite geliştirme süreci ve topluluğa devam eden bir katılımın ardından, okulların kendilerini hazır hissettiklerinde öz değerlendirme formuna geçebilecekleri, değerlendirme formunun bir dizi sorudan oluştuğu, alacağınız puanlara göre (Ve ayrıca, kaynaklar, olay durumları ve topluluk üzerindeki faaliyetler yoluyla katkınızı dikkate alarak) bir uzmanın faaliyetlerinizi gözden geçireceği ve bir etiket (Demir, Bronz, Gümüş veya Altın) alabileceğiniz sayfada anlatılmaktadır.

43. Collaborate:"İşbirliği" sekmesinde eSafety Etiket Topluluğuna katılmak, çevrimiçi güvenliğe ilişkin görüş ve bilgilerinizi arkadaşlarınızla paylaşmanıza olanak tanındığından, bu alanda uzmanlığınızı ve düşüncelerinizi diğer topluluk üyeleri ile paylaşabileceğinizden, sorular sorup veya başkalarının deneyiminden yararlanabileceğinizden bahsedilmektedir.

44. Bu sayfada anket ekranı, forum bölümü özet ekranı ve blog sayfası ekranı bölümleri bulunmaktadır.

45. Get label:"Etiket al" sekmesinde eSafety label etiketini nasıl alabileceğinize dair bir rehber bulunmaktadır. Zaman çizelgesi bölümünde, akreditasyon sürecinin ne kadar sürdüğünü daha iyi anlamanızı sağlayacak bilgi grafiği vardır. Türkçeye çevirdiğim bilgi grafiğine buradan ulaşabilirsiniz.

46. Daha üst seviye etiket alabilmek için ne zaman ve hangi koşullar altında yeniden başvuru yapmanız gerektiği de yine ilgili grafikte anlatılmıştır. Ayrıca bu bölümde değerlendirme formunun üç kategoriden (Altyapı, politika ve uygulama) ve 30 sorudan oluştuğu da söz edilmektedir.

47. Bu bölümde etiket süreci temelde 3 adım şeklinde detaylı anlatılmıştır. Bunlar 1. Hazırlık, 2. İletişim kurma, katılım sağlama, katkıda bulunma, 3. Değerlendirme Formunu doldurma şeklindedir.

48. Resources:"Kaynaklar" sekmesinde çevrimiçi güvenlik kaynakları, modern teknolojinin ve çevrimiçi araçların okullarda güvenli kullanımı hakkında farkındalık yaratmayı veya rehberlik sağlamayı amaçlayan materyallerden söz edilmektedir. Kaynaklar bölümüne videolar, broşürler, kitapçıklar, atölyeler, ders planları, kampanyalar, araçlar, eTwinning projeleri, posterlerin yüklenebileceği belirtilmektedir.

49. Kaynakların yüklenmesi, diğer öğretmenlerin daha güvenli bir çevrimiçi ortam oluşturmasına yardımcı olacak ve okulunuzun eSafety Etiketi akreditasyonu için ekstra puan kazanacağınız açıklanmaktadır.

50. Sayfa da "Bir kaynak yükle" bölümü de bulunmaktadır.

51. Cases:"Vakalar" bir okulda meydana gelen gerçek bir olayın ve bunun nasıl çözüldüğünün raporlamasından bahsedilmektedir. Okulunuz, siber zorbalık, kötü amaçlı yazılımların sisteme bulaşması veya gizliliğin ihlali gibi çevrimiçi bir güvenlik olayı yaşadı mı, bu tür durumlarla nasıl başa çıktınız? gibi sorular da ele alınmaktadır.

52. Okulunuzda meydana gelen bir olayı eSafety portalına bildirmeniz ve eSafety portalı'nın benzer durumlarla karşı karşıya kalan diğer öğretmenlere yardımcı olabilecek bir olay galerisi oluşturmasına yardımcı olmanız istenmektedir. Okulunuzun eSafety Etiketi akreditasyonu için vakalar bölümünün önem taşıdığından söz edilmektedir.

53. Sayfa da "Bir vaka bildir" bölümü de bulunmaktadır.

54. eSafety Label platformu eğitim alanında birçok paydaşı ile eğitim alanında işbirliği, güç birliği içindedir. Bu paydaşlardan "European SchoolNet" eTwinning öğretmenlerinin yakından tanıdığı stratejik ortaktır.

Kaynaklar bölümüne videolar, broşürler, kitapçıklar, atölyeler, ders planları, kampanyalar, araçlar, eTwinning projeleri, posterlerin yüklenebileceği belirtilmektedir.

Cases:

"Vakalar" bir okulda meydana gelen gerçek bir olayın ve bunun nasıl çözüldüğünün raporlamasından bahsedilmektedir. Okulunuz, siber zorbalık, kötü amaçlı yazılımların sisteme bulaşması veya gizliliğin ihlali gibi çevrimiçi bir güvenlik olayı yaşadı mı, bu tür durumlarla nasıl başa çıktınız? gibi sorular da ele alınmaktadır.

Okulunuzda meydana gelen bir olayı eSafety portalına bildirmeniz ve eSafety portalı'nın benzer durumlarla karşı karşıya kalan diğer öğretmenlere yardımcı olabilecek bir olay galerisi oluşturmasına yardımcı olmanız istenmektedir. Okulunuzun eSafety Etiketi akreditasyonu için vakalar bölümünün önem taşıdığından söz edilmektedir.

Sayfa da "Bir vaka bildir" bölümü de bulunmaktadır.

eSafety label portalında ana sayfa üzerinde yer alan "Login" sekmesi tıklanıp üyelik işlemleri bölümüne girilir. Bu portal üzerinde şu an itibarı ile Türkçe dil desteği bulunmamaktadır. Bu yüzden tüm süreç seçilen dile göre işleyecektir.

Login sekmesinden ekrana EUN ID login bölümü gelecektir. Daha önce European SchoolNet üzerinden bir şifre alındıysa aynı şifre burada da kullanılabilir. Eğer alınmadıysa, ilk defa üyelik gerçekleşecek ise "Create an account" tıklanır.

Register (Kayıt) aşaması oldukça kolaydır. Username (Kullanıcı adı) bölümüne takma isim veya en kolay akılda kalacak haliyle ad ve soyad Türkçe karakter kullanılmadan bitişik yazılır. "First name" bölümüne ad, "Family name" bölümüne soyad yazılır. "Email" bölüne elektronik posta, "Password" bölümüne alfanumerik yani harf ve sayılardan oluşan mümkünse 8 haneli bir şifre belirlenerek yazılır.

reCaptcha yeni nesil güvenlik anahtarıdır. "I'am not a robot" butonu tıklanır. Ekrana gelen soruya uygun resimler tıklanarak güvenlik aşaması geçilir.

Son olarak "I declare that I have read and accept the EUN Partnership AISBL legal statements and privacy policy" butonu tıklanır. "Submit" yani gönder butonuna tıklanarak üyelik giriş işlemi başlatılır.

Sisteme giriş yapıldıktan sonra ekrana "User profile" kullanıcı profili bölümü gelir. Bu bölüme tıklanarak kullanıcı bilgileri bölümüne gidilir.

Kullanıcı bilgileri bölümü açıldığı zaman sol üst tarafta bulunan "Edit profile" profili düzenle sekmesi tıklanır.

Yeni açılan pencerede detaylı profil düzenleme sayfası açılır. Kullanıcı isminin yanında bulunan "Edit" yazısına tıklanarak detay profil sayfasına geçilir.

Bu aşamada "Salutation" selamlama bölümüne bay, bayan benzeri ön tanımlama yazılır. "First name" ad, "Family name" soyad otomatik olarak ekrana gelir. "Country" bölümünden ülke seçilir. "Mother tongue" bölümünden ise anadil seçilir. "Other spoken languages" diğer konuşulan diller bölümünden istenirse farklı dilde eklenebilir. "Describe yourself" kullanıcının kendi hakkında kısa bir öz geçmiş yazma bölümüdür. "Website" bölümüne okul web adresi yazılır.

"I would like to receive news or invitations from European Schoolnet" Avrupa okul ağı ile ilgili haberleri almak isterim butonu tıklanması tavsiye edilir.

"Submit" yani gönder butonuna tıklanarak üyelik bilgileri güncelleme işlemi tamamlanır.

Tekrar profili düzenle bölümüne gelinir. Bu noktada "My organisations" organizasyonlarım bölümünün altında "Add" ekle kelimesinin üzerine gelinerek tıklanır.

Açılan pencerede "Select your organisation" organizasyonunuzu seçin penceresi çıkacaktır. "Country" bölümünden ülke adı, "Region" bölümünden şehir, "Town" bölümünden ilçe adı seçilir. Daha sonra bu ilçede kayıtlı okulların listesi otomatik olarak açılacaktır.

Eğer kullanıcının okulu açılan seçeneklerde gözüküyorsa o okulun yanında bulunan "This is my organisation" ifadesi tıklanır ve okul kullanıcı profiline eklenir. Eğer kullanıcı okul ismini bulamıyor veya ilk defa kayıt oluyorsa "I did not see my organisation in the list" yani bu listede okulumu göremedim/bulamadım butonunu tıklayıp okulunu kayıt etmek zorundadır.

Yeni okul eklemek:

“Official institution name” okulun resmi adıdır. “Address” okulun adresidir. “Town” okulun bulunduğu ilçedir. “Post code” okulun adresine bağlı posta kodudur. “Country” okulun bulunduğu ülkedir. “Region” okulun bulunduğu ilçedir. “Website” bu alana okul web sayfasının ismi yazılmalıdır. “Number of pupils” bu alana okuldaki öğrenci sayısı yazılmalıdır. “Minimum age of pupils” bu alana en küçük öğrenci yaş grubu girilmelidir. “Maximum age of pupils” bu alana en büyük öğrenci yaş grubu girilmelidir. “Telephone” okulun telefon numarası numaranın başına +90 getirilerek yazılmalıdır. “Email” okulun resmi elektronik posta adresi yazılmalıdır. “Fax” okulun var ise fax numarası numaranın başına +90 getirilerek yazılmalıdır.

“Area” bölümünden okulun bulunduğu alan seçilmelidir. Genel olarak “Urban” kentsel seçeneği tercih edilir. “Specialisation” uzmanlaşma alanından okulun nitelikleri işaretlenir. İstenilirse birden fazla seçenek işaretlenebilir. “Sector” kısmından okulun “Private” özel mi yoksa “Public” devlet okulumu olduğu tercih edilebilir. “Description” açıklama kısmında okul ile ilgili ek bilgiler verilebilir. “About what you do” kısmı kullanıcının okulda hangi unvanı taşıdığına ilişkindir. “Role” bölümünden kullanıcının resmi görevi seçilir.

“Submit changes” yani değişiklikleri gönder butonuna tıklanarak üyelik bilgileri güncelleme işlemi tamamlanır.

Kapasite geliştirme eSafety etiketini edinmede ilk adım olsa da, tüm süreç boyunca devam etmekte ve okulların akranlar ve uzmanlarla bilgi alışverişinde bulundukları, tavsiye talep ettikleri ve kişisel deneyimlerinden örnekler sağladıkları katılım aşaması ile tamamlanmaktadır. Bütün bunlar, eSafety etiketi Topluluk’ta (Bloglar, Forumlar, Anketler, Elçilerin Bölümü) bulunan çeşitli iletişim araçlarıyla sağlanır.

Bir eSafety etiketi edinme süreci Hazırlık, Topluluk ve Akreditasyon olarak 3 aşamalı bir süreçten sonra oluşur.

Kapasite geliştirme süreci ve topluluğa devam eden bir katılımın ardından, okullar kendilerini hazır hissettiklerinde öz değerlendirme formuna geçebilirler. Değerlendirme formu bir dizi sorudan oluşur. Alacağınız puanlara ve ayrıca, kaynaklar, olay durumları ve topluluk üzerindeki faaliyetler yoluyla katkınızı dikkate alarak, bir uzman faaliyetinizi gözden geçirecek ve Demir, Bronz, Gümüş veya Altın etiketlerinden birini size verecektir.

Forma Erişim:

eSafety Label ana sayfasında sağ üst köşede bulunan kullanıcı adı tıklanır.

Açılan profil sayfasında “My role & organisations” kategorisinden okulun adı tıklanır.Açılan sayfada “Our assessment” okulun değerlendirme bölümünde “Edit assessment” tıklanır.

Eğer okulun daha önce hiçbir kaydı yoksa “You have an assessment which has not been submitted yet.” Henüz bir değerlendirme gönderilmemiş uyarısı çıkar.

Bu aşamadan itibaren form butonu tıklanıp değerlendirme formuna giriş yapılır.

Önemli not: Okulunuzu sisteme tanımlamadığınız zaman değerlendirme formunu ekranda göremezsiniz.

Açılan değerlendirme formu 4 ana başlıktan oluşmaktadır.

1. “Infrastructure”: Altyapı

2. “Practice”: Uygulama

3. “Policy”: Politika

4. “User guidance”: Kullanıcı rehberi

eSafety Label değerlendirme aracı, okulun bilişim teknolojisini kullanımı açısından nerede durduğunu göstermeyi amaçlar ve hem öğrenciler hem de personel için en uygun yetkiyi ve güvenliği geliştirmede destek olacak bir “Eylem Planı” sunar.

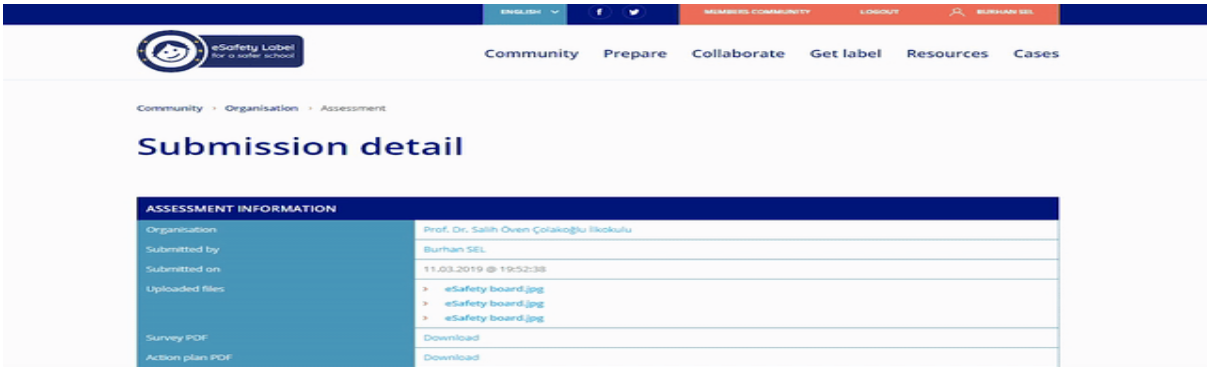
Kullanıcı rehberi, altyapı, politika ve uygulama ile ilgili konuları kapsayan rastgele seçilmiş 30 değerlendirme sorusundan oluşmaktadır.

Soruların tamamlanmasının ardından, öğretmenlere, öğrencilere ve okulun yöneticilerine danışılmalıdır. Bunların hepsi okul ortamı üzerinde güçlü bir etkiye sahiptir.Tüm sorulara cevap verdikten sonra, “Gönder” düğmesini tıklayarak yanıtları göndermek gerekir.

Eylem Planı otomatik olarak oluşturulacak ve istenildiği zaman indirilebilecektir. Bu “Eylem Planı”, okuldaki bu önemli performans alanında mükemmelliğe ulaşmaya yardımcı olmak için iyi bir rehber ve kaynak olacak, aynı zamanda diğer okullarla irtibat kurulmasına katkı sağlayacaktır.

Değerlendirme sonuçlarına göre okullar Bronz, Gümüş veya Altın etiket olarak akredite edilecektir. Eylem Planında belirlenen görevleri tamamlayarak bir sonraki seviyeye geçmek mümkündür. Etiket 18 ay boyunca geçerli olmakla birlikte, sertifikayı değişim hızıyla geçerli tutmak için her yıl eSafety Label sertifikasının yenilenmesi tavsiye edilir.

E-Güvenlik etiketi web sitesinde, "eSafety bilgi formları" bölümünde, Altyapı, Politika ve Uygulama ile ilgili çok çeşitli konular bulunmaktadır. Bu konular okulun değerlendirme formunu doldururken kullanıcıya yardımcı olabileceği için eksiksiz olarak okunmalıdır.



Önemli İp Uçları:

- Her bölümün sorularının cevaplanması zorunludur. Soruların seçenekleri seçildiği zaman mutlaka o sorunun altında bulunan "Submit answer" cevabı kaydet seçeneği seçilmelidir. Genel olarak tüm soruların altında olan "Further Comments" diğer yorumlar kutucuğuna istenilen ifadeler de yazılabilir.
- Sorular her kullanıcı için rastgele soru havuzundan seçilmektedir. Kullanıcılara sorulan soru örneklerine etik değerler gereği bu eğitimde yer verilmemiştir, örnek olarak birkaçı seçilmiştir.
- Tüm sorular kullanıcının sistemde seçtiği dilde geldiği için o dil konusunda uzman bir kişiden destek alınabilir. Türkçe dil seçeneği eğitim yayına hazırlandığı tarih itibarı ile sistemde bulunmamaktadır.
- Soruların sadece formu dolduran kullanıcı tarafından değil, okul yönetimi ile işbirliği içinde doldurulması ve cevaplanması gerekmektedir.
- Okulda kullanılan bilgisayarların virüs koruma yazılımlarının olup olmaması ve yönetimi, okul modem ve ağ altyapısının güvenliği ve güncelliği, okul ağ erişiminin sosyal medya kaynaklarına erişip erişmediği gibi konularda okulda bilişim teknolojileri yetkinliği olan bir eğitimci varsa ondan, yoksa mutlaka profesyonel bir bilişim teknolojileri uzmanından destek alınmalıdır.
- Okul SWOT analizlerinde, stratejik planlarında, öğretmenler kurul toplantılarında e-Güvenlik ile ilgili güncel politikalar işlenmeli ve gündeme alınmalıdır. Okul öğretmen

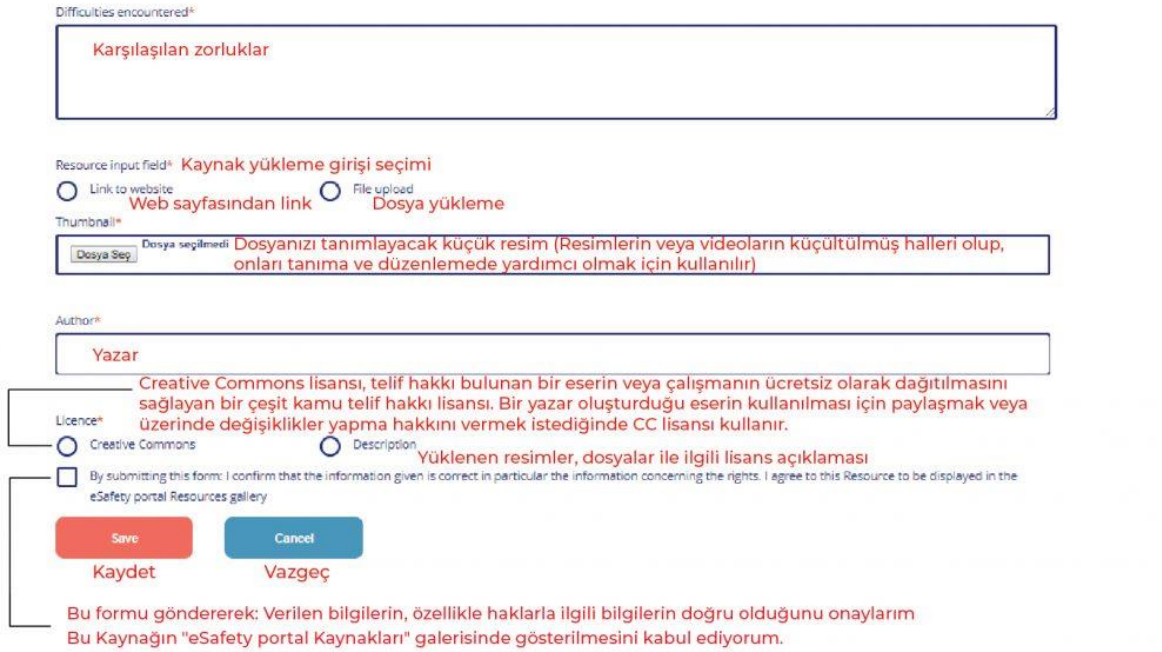
ve öğrencilerinin e-Güvenlik konusunda duyarlı ve bilinçli olmaları, bilgilerini okul yönetimi kılavuzluğunda sürekli güncel tutmaları önemlidir.

- "Action plan pdf" bölümünden okul hareket eylem planı indirilebilmektedir.
- "Survey pdf" bölümünden, formda sorulara verilen cevaplar incelenebilmektedir.
- "View Submission results" bölümünden gönderim detayları takip edilebilmektedir.
- "View uploaded files" bölümünden sisteme yüklenen dosyalar incelenebilmektedir.

ASSESSMENT INFORMATION	
Organisation	Kurum adı
Submitted by	Kim tarafından formun yüklendiği
Submitted on	Formun yüklendiği tarih ve saat
Uploaded files	Sisteme yüklenen dosyalar
Survey PDF	Formda size sorulan sorular ve cevaplarınız (İndirilebilir)
Action plan PDF	Sistem tarafından oluşturulan aksiyon planı (İndirilebilir)
POINTS	
ASSESSMENT	
Infrastructure score	Alt yapı puan değerlendirmeniz
Policy score	Politika puan değerlendirmeniz
Practice score	Uygulama puan değerlendirmeniz
Bonus score	Kaynaklar ve vaka inceleme bölümüne katkınız, forum ve blog sayfalarına katılımınız, okul aksiyon planında ki eksiklerinizi her geçen başvuru döneminde geliştirmeniz
Total score	Toplam puanınız
Label	Değerlendirme sonucu okulunuza tanımlanan etiket

Dip Not:

- *Son olarak profil bölümünden okul adı tıklandığı zaman okulun aldığı eSafety etiketi çıkmaktadır. Okul web sayfasına bağlantı (Linkleme) yapılacağı zaman "Embed label" linkinden alınan verideki html kodları silinip örneğin: "http:// storage.eun.org/esafety-label-medal/Bronze_2017_11_en_b7249.png" şeklinde yazılmalıdır. (Tırnak işaretleri olmaksızın)*
- *Okul web sayfasına eSafety etiketini eklemek ve bağlantı vermek için fare imleçi etiketin üzerinde iken sağ tıklanıp, resmi farklı kaydet seçeneği ile resim kayıt edilebilmektedir.*

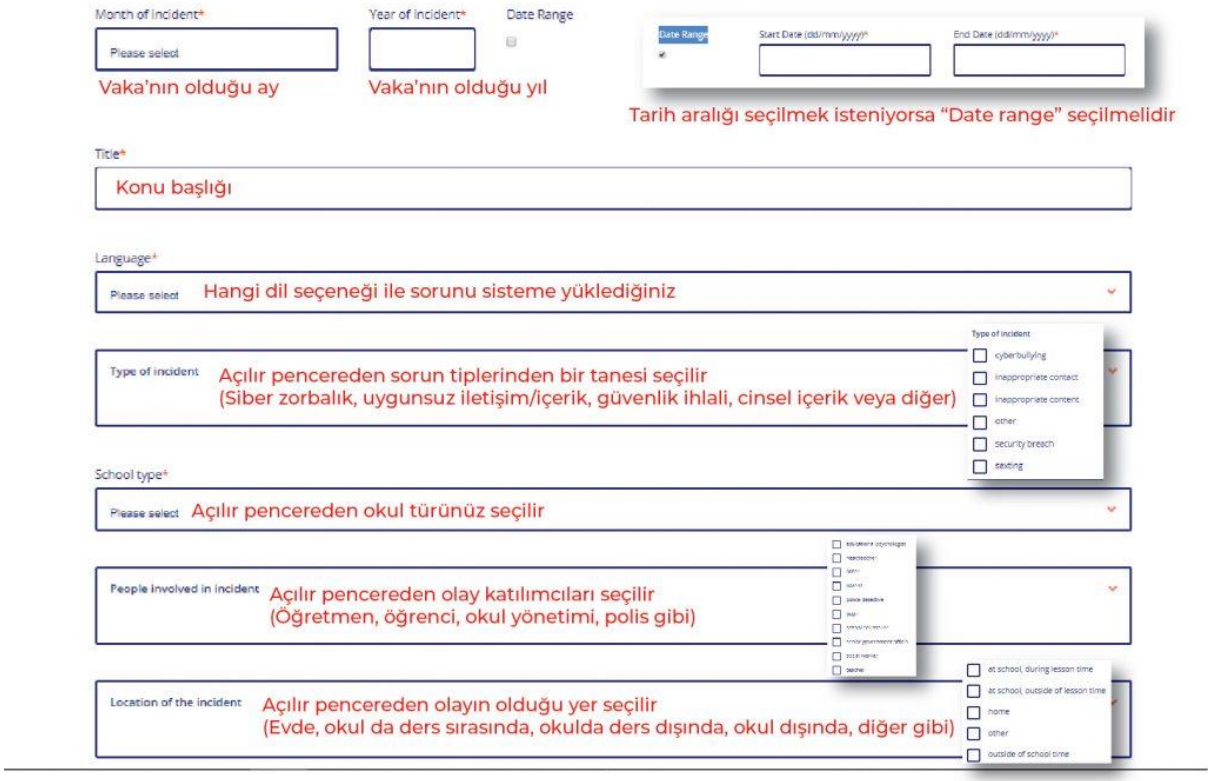


Vaka incelemesi, e-Güvenlik ile ilgili okulda öğrencilerin veya personelin yaşadığı sorunların raporlandığı ve sisteme yüklendiği bir bölümdür.

Sisteme kayıtlı olan eğitimcilerin, diğer meslektaşlarının benzer durumlarda sorunlara nasıl çözüm bulduklarını veya sorunları nasıl tanımladıklarını görmeleri açısından önemli bir bölümdür. Sorunlar ve çözüm yolları hakkında bilgi ve deneyim paylaşımı olması bu bölümü daha da önemli hale getirmektedir.

Vaka formu oluşturmasında dikkat edilmesi gereken nokta, formda açılan tüm sorulara cevap verme ve formun altında bulunan form gönderme onay butonunun işaretlenmesi gerekliliğidir.

Form bölümleri:



Son olarak mutlaka kullanım sözleşmesi onaylanmalıdır.

Okul Aksiyon Planı, değerlendirme formu sonucu ne olursa olsun okulunuzun gelişimi için sistem tarafından hazırlanan "Okula özel" bir plandır.

Planda okulun güçlü ve zayıf yünlerinin analizleri, değerlendirme formunda verilen cevaplara göre yapılmaktadır. Aksiyon planında tavsiyeler ve okulun var olan durumu detaylı olarak tanımlanmaktadır.

Plan, değerlendirme formunda size sorulan ve soru havuzundan rastgele seçilen sorulara verdiğiniz cevaplara göre şekillenir.

Örnek Okul Aksiyon Planı Bölümleri ve İçerikleri:

Bu örnek eylem planı tam metni sizin değerlendirme formunu daha iyi kavramanıza, okulunuzun e-Güvenlik alanında farkındalık yaratma yolunda ilerlemesine imkan sağlayacaktır.

eSafety Etiketi – Eylem Planı

"… okulu için … tarafından sunulan eylem planı – *tarih @ saat"*

"Doldurulmuş "Değerlendirme Formunu" eSafety Etiketi portalına göndererek, okulunuzdaki eSafety'nin durumunu analiz etmek için önemli bir adım attınız. Lütfen eSafety'yi okulunuzda daha da iyileştirmek için ve neler yapabileceğinizi görmek için Eylem Planınızı dikkatlice okuyunuz. Eylem Planı, 3 temel alana bölünmüş faydalı öneriler ve yorumlar sunar: Bunlar Altyapı, politika ve uygulama bölümleridir."

Altyapı

Teknik Güvenlik

– Tüm okul cihazlarınızın virüs korumalı olması tavsiye edilir. Hem okul politikanıza hem de "Kabul Edilebilir Kullanım Politikanıza" virüs koruması ile ilgili bir paragraf eklediğinizden ve personelin ve öğrencilerin okul kurallarını titizlikle uyguladıklarından emin olmalısınız.

– Kullanıcılardan kendi web filtrelemelerini tanımlamaları istense de ve bu sorumlu kullanımı teşvik etmek için iyi yol olsa da, çoğu öğrenci kullanmaları gereken filtreleme seviyesi hakkında bilinçli bir karar verebilecek kadar olgun değildir. Okul veya en azından öğretmenler, hangi düzeyde filtrelemenin kullanılacağına karar vermelidirler. Öğrencilerin ebeveynleri tipik olarak filtrelemenin okul veya öğretmen tarafından yapılmasını tercih eder; çünkü gençler, potansiyel olarak zararlı ya da yasa dışı olsun, kazayla neyle karşılaşabileceklerinin farkında değillerdir. Bununla birlikte, her yaştaki öğrencilere bir eğitim yaklaşımı ve esneklik kazandırmak da güvenli ve sorumlu çevrimiçi kullanımın anahtarıdır. Bu nedenle tüm öğretmenleri, iyi ve güvenli bir dijital vatandaş olma konusunda öğrencileriyle nasıl konuşacakları hakkında bir fikir fırtınası yapmak için bir araya getirmelisiniz.

Öğrencilerin ve Personelin Teknolojiye Erişimleri

– Okul çalışanlarının ve öğrencilerin okul bilişim araçlarında USB bellek kullanabilmelerine dair yeterli eğitim almaları gerekmektedir. Bu konuda personelinize ve öğrencilerinize izin verirken onları güvende tutmak için, Kabul Edilebilir Kullanım Politikanıza temel kuralları da eklemeniz gerekir.

– Her akademik yılın başında öğrencilerle e-Güvenlik tanımları hakkında konuşulmalı, böylece kendilerini ve mahremiyetlerini korumak için neyin doğru neyin yanlış olduğunun daha çok farkına varmaları sağlanmalıdır.
Okul politikanızı teknoloji yerine davranışa dayandırın. Ziyaretçiler okulun ağını kullanmadan önce Kabul Edilebilir Kullanım Politikasını okumalı ve imzalamalıdır.

Veri koruması

– Öğrenme ve yönetim ortamlarınızı ayrı tutma konusunda mutlaka politikanız olmalıdır. Politikalarınızı incelemeye devam ederken bu ortamları yönetme konusunda eğitim almış personelin bilgilerinin güncel olması sağlanmalıdır. Ayrıca politikanızı okul profilinize yükleyerek diğer eSafety Etiket kullanıcılarıyla paylaşabilirsiniz.

– E-posta sisteminizin korunması ve öğrenci verilerinin aktarılması konusunda bir politikanız olmalıdır. Bu bakımdan, tüm personelin okul bilgisayarlarından ulaşmaları muhtemel uygunsuz veya yasadışı içerik bulmaları durumunda ne yapmaları gerektiği konusunda net olmaları için kılavuzlar hazırlamanız önemlidir.

Yazılım Lisansı

– Tüm okul personelinin, yazılım lisansları konusunda bilgilendirilmesinin sağlanması önemlidir. Bu, sistemlerinizin güvenliğinin sağlanabileceği ve personelin öğretme ve öğrenmeye yardımcı olacak yazılım uygulamalarını deneyebilecekleri anlamına gelecektir.

– Yüklü yazılımlara ve lisanslara kısa bir zaman dilimi içinde birkaç kişinin yardımıyla bir denetleme sistemi geliştirmeniz tavsiye edilir.

Bilişim Teknolojileri (BT) Yönetimi

– BT ağından sorumlu olan kişinin okula ait donanımı konusunda tam olarak bilgilendirilmesini sağlamak ve bunun Okul Politikası ve Kabul Edilebilir Kullanım Politikası'nda açıkça belirtilmesi gerekir. Ağdan sorumlu olan kişinin lisans sorumluluklarına dikkat etmesi gereklidir. Okulunuzda yalnızca okul yöneticileri ve / veya BT sorumlusu yeni yazılımlar alabilir.

– Okul yönetimi öğretmenlerin okul bilgisayarlarına/etkileşimli tahtalarına yeni yazılımlar isteyebilecekleri bir sistem kurmayı düşünmelidir. Bu yeni yazılımlar, öğretmenlere derslerde daha ilgi çekici ders oluşturmalarına imkan sağlar.

Politika

Kabul Edilebilir Kullanım Politikası (AUP)

– Okul topluluğunun tüm üyeleri için Kabul Edilebilir Kullanım Politikanız olması gereklidir. AUP'a okulunuzun uygun olduğundan emin olmak için okul politikalarınızı düzenli olarak gözden geçirmelisiniz.

– Okulunuzda e-Güvenlik ile ilgili bir değişiklik yapıldığında okul politikalarının gerektiğinde revize edilmesi iyi bir uygulamadır. Bununla birlikte, okul dışındaki değişikliklerin de yeni yasalar veya değişen teknolojiler gibi politikaları etkileyebileceği unutulmamalıdır. Bu nedenle, lütfen politikalarınızı en az yılda bir kez gözden geçirin.

Raporlama ve Olay İşleme

– Tüm personel, potansiyel olarak yasa dışı olabilecek materyallerle başa çıkma prosedürünü bilmelidir. Bu tür bir durumda genel sorumluluk alabilecek okul üst düzey liderlik ekibinden bir isim seçilmelidir. Prosedür, Okul Politikasındaki tüm personele ve Kabul Edilebilir Kullanım Politikasındaki personel ve öğrencilere açıkça iletilmelidir. Ulusal INHOPE yardım hattınıza (www.inhope.org) yasadışı içerik bildirmeyi ve şüphelendiğiniz durumları bildirmeyi unutmayın. Türkiye için ihbarweb.org.tr sayfasından raporlama yapılabilir.

– Zorbalık olaylarına uygulanan detayları ve çözümleri hem çalışanlar hem de eSafety Label olay işleme formu aracılığıyla paylaşmalısınız. Ancak bu şekilde deneyim kazanabilir ve başkalarının benzer olayları ele alma uygulamalarını öğrenebilirsiniz. Ayrıca, Kabul Edilebilir Kullanım Politikanızdaki zorbalıkla mücadele kurallarının öğrencilere ve personele iletildiğinden emin olmalısınız.

Personel Politikası

– Yeni personel de dahil olmak üzere, tüm personelin çevrimiçi davranışlarla ilgili politikadan haberdar olmalarını sağlamalısınız. Bu, personel toplantılarında düzenli olarak tartışılan ve Okul Politikasında açıkça kabul edilen ve Kabul Edilebilir Kullanım Politikasındaki personel ve öğrencilere açık bir konu olmalıdır. Her iki belgeyi de düzenli olarak gözden geçirmeli ve güncellemelisiniz.

– Okulunuzda kullanıcı hesapları doğru olarak yönetilmelidir. Bu, yanlış kullanım riskini azaltması açısından önemlidir.

Öğrenci Uygulaması / Davranışları

– Öğrenciler için elektronik iletişim kuralları Kabul Edilebilir Kullanım Politikasında açıkça belirtilmelidir. Standartlar belirlenmemişse öğrenciler arasındaki iletişim, siber zorbalık gibi olaylara yol açan etkenler hızlı bir şekilde artabilir. Etkili ve sorumlu bir iletişim kurmayı öğrenmek, her genç için gerekli bir yeterlilik ve okul müfredatının da bir parçası olmalıdır. Uygulamak istediğiniz standartları tanımlamak için bir personel/öğretmenler toplantısında bunu mutlaka gündeme getirmelisiniz.

– Okulunuzdaki eSafety uygulamaları tartışılırken, öğrencilerden geri bildirimler gelebilir. Öğrencileri mümkün olduğu kadar işleyişe dahil edin, böylece öğrenciler gerçek hayattaki sorunları daha yakından tanırlar.


eSafety Label - Action Plan

Action plan submitted by Burhan SEL for Prof. Dr. Salih Özen Çolakoğlu İlkokulu - 11.03.2019 @ 19:52:37

By submitting your completed Assessment Form to the eSafety Label portal you have taken an important step towards analysing the status of eSafety in your school. Congratulations! Please read through your Action Plan carefully to see what you can do to improve eSafety further in your school. The Action Plan offers useful advice and comments, broken down into 3 key areas: infrastructure, policy and practice.

Infrastructure

Technical security

- It is very good that all your school devices are virus protected. Make sure you also have included a paragraph on virus protection in both your school policy and your Acceptable Use Policy, and ensure that staff and pupils rigorously apply school guidelines. If you need further information, check out the fact sheet on Protecting your devices against malware at www.esafetylabel.eu/group/teacher/protecting-devices-against-malware

Online Okul Varlığı

– Okul Politikanızın tüm alanları kapsadığını göstermek için okulda fotoğraf ve videoların izinsiz çekilmesi ve yayınlanması hakkındaki politikanızı öncelikle hayata geçirin.

– Okulunuzun çevrimiçi itibarını kontrol edecek bir okul yöneticisinin veya öğretmeninin olması tavsiye edilir. Okuldan erişim izni olan, yeni açılan bazı web sayfalarının olumsuz içerikler sunmaları durumunda özellikle okullara, öğrencilerine ve çalışanlarına zarar verebileceklerinden, bu sitelerden haberdar olun ve bunları periyodik olarak izleyin.

Uygulama

eSafety Yönetimi

– Gerekli tüm ağ güvenliği ve kullanıcı gizlilik kontrollerinin yapıldığından emin olunmalıdır. Okulların düzenli aralıklarla denetim ve prosedür kontrolleri yapmaları şarttır. Her zaman eSafety konusunda genel bir lider kişi olmamasına rağmen, okuldaki herkes günlük işlerinde kullanılan hassas bilgileri korumak için ortak bir sorumluluğa sahiptir. Doğrudan veri işleme ile ilgisi olmayan personel bile, riskler ve tehditler ve sorunların en aza nasıl indirileceğinden haberdar edilmelidir. Okuldaki herkes olabilecekleri en iyi ve en güvenli dijital vatandaşlar olmaları konusunda sürekli olarak eğitimden geçmelidir.

– Okulunuzdaki tüm personelin eSafety'den sorumlu olması tavsiye edilir. Ancak, gerekli odağı sağlamak için eSafety konularında genel sorumluluğu olacak bir kişi (Örneğin okul yöneticilerinden biri) tayin etmek gereklidir. Bu kişi Okul Politikanızı geliştirirken ve düzenli olarak gözden geçirirken sorumlu olmalıdır.

Müfredatta eSafety

– eSafety'nin ülkenizde yasal bir zorunluluk olup olmadığına bakılmaksızın tüm müfredata dahil edilmesi gerekir.

– Ortaya çıkan sorunlara ayak uydurabilen bir eSafety müfredatı sağlayabilmeniz önemlidir. Okul profilinize, müfredatı nasıl tasarladığınızın bir taslağını ve kullandığınız kaynakların bazılarıyla ilgili bağlantılar verebilirsiniz. Bu, diğer okullar için oldukça yararlı olacaktır.

Müfredat Dışı Etkinlikler

– Öğrencilere, istendiğinde müfredat süresi dışında eSafety desteği sağlamanız tavsiye edilir. Tüm öğrencilere çevrimiçi güvenlik sorunlarıyla başa çıkmak için destek sunmanız önemlidir. Öğrencilere okul dışında çevrimiçi teknolojiyi kullanmaları hakkında mutlaka eğitim verilmelidir.

– Öğrencilerinizin çevrimiçi alışkanlıklarıyla ilgili bilgilerini eSafety Etiketi topluluğu aracılığıyla diğer okullarla paylaşabilirsiniz. Örneğin, öğrencilerin çevrimiçi alışkanlıklarına ilişkin en son anket bulgularınızı okul alanınıza okul profilinize yükleyebilirsiniz.

Destek Kaynakları

– Tüm personelin eSafety için bir sorumluluğu olmalıdır. Okul rehber öğretmenleri e-Güvenlik konularında tavsiye ve rehberlik sağlamak için iyi bir konumdadır. Okul Politikanızı geliştirmeye ve düzenli olarak gözden geçirmeye katkıda bulunmak için okuldaki diğer personeller toplantılara davet edilmelidir.

– Okulunuzdaki öğrencilerin aktif olarak eSafety mentoru olmaları için teşvik edilmesi tavsiye edilir. Bu ağın güçlendirilmesi konusundaki yaklaşımınızı forum veya okulunuzun profil sayfası aracılığıyla eSafety Label web sitesindeki diğer öğretmenlerle paylaşabilirsiniz.

Personel Eğitimi

– eSafety konularında ortaya çıkan trendler hakkında tüm personelin düzenli olarak bilgilerinin güncellenmesi gerekir. Personelin eğitimlerinde neye ihtiyaçları olduğunu belirlemek için mutlaka bir ihtiyaç analizi yapın.

– Okulunuzda personel üyeleri arasındaki bilgi alışverişi teşvik edilmelidir. Bu, tüm okul için faydalı olacaktır. "Okul alanım" aracılığıyla da erişilebilen yükleme aracı aracılığıyla eSafety konularında PowerPoints, belgeler veya benzer bilgileri sisteme yükleyin.

"Gönderdiğiniz değerlendirme formu büyük bir soru havuzundan oluşturulmuştur. Ayrıca ankette bahsedilmeyen alanlarda eSafety'yi geliştirip geliştirmediğinizi bilmek de bizim için yararlıdır. Bu tür değişikliklerin kanıtlarını eSafety Portalının Okul alanım bölümüne yükleme kanıtı aracılığıyla yükleyebilirsiniz.

Unutmayın, Değerlendirme Formunun doldurulması Akreditasyon Sürecinin sadece bir kısmıdır, çünkü kanıtların yüklenmesi, Forum aracılığıyla başkalarıyla görüş alış-verişiniz ve verilen şablondaki olayları bildirmeniz değerlendirmede dikkate alınır."

eSafety Label +: Bir sonraki eSafety şampiyonu olun siz olun!

"Bir sonraki eSafety Şampiyonu Olun" sloganı ile yola çıkan eSafety Label+, geniş bir Avrupa öğretmenler topluluğu ve diğer okul aktörleri arasında bilgi alışverişini ve en iyi uygulamaların değişimini teşvik etmek, okulları daha güvenli ve sorumlu bir dijital gelecek için donatmak için hazırlanmış bir Erasmus+ projesidir.

Eğitimde e-Güvenlik:

Eğitimde çevrimiçi güvenlik gereksinimlerinin ve önceliklerinin haritalandırılması için eSafety Label tarafından bir araştırma raporu hazırlanmıştır.

Rapor neyi başarmayı hedeflemiştir?

eSafety Label + projesinin ana sonuçlarından biri olan bu rapor, Avrupa genelindeki okullarda çevrimiçi güvenliğin temel, güçlü ve zayıf yönlerini belirlenmesine ve iyileştirme alanlarının öğrenilmesine olanak sağlamıştır. Ayrıca, eSafety Label'in mevcut sertifikalandırma sürecini ve bu girişimin okul ortamındaki etkisinin değerlendirilmesini sağlamıştır.

Rapor, eSafety Label topluluğunun 1.150 üyesi arasında yapılan kantitatif bir araştırmaya dayanmış ve tüm eSafety Label + proje etkinlikleri için bir temel oluşturmuştur.

eSafety Label + hakkında detaylı bilgi için burayı veya aşağıdaki eSafety Label + logosunu tıklayınız.

Sonuç olarak bu araştırmalar, okulların ihtiyaç ve güçlerini çevrimiçi güvenlik açısından geliştirmeleri için şu adımların atılması gerektiği ortaya çıkarmıştır:

1. eSafety Etiketi akreditasyon süreci öğretmenler ve diğer okul personeli için kolaylaştırılmalı,

2. eSafety Label topluluğu tarafından sağlanan bilgilerin kapasitenin geliştirilmesinde daha iyi hale getirilmesi için çalışılmalı.

3. Okul personeli için eSafety adımlarının anlatıldığı rehber geliştirmek.

Raporda ortaya çıkan ana çıktılar ve öneriler:

Genel olarak, bu araştırmanın dayandığı anketin sonuçları çok olumlu olmuştur. Katılımcıların çoğunluğunun değerlendirme formu ile ilgili bir iyileştirmenin gerekli olmadığını düşündükleri ortaya çıkmıştır. Bu, bir eSafety etiketi edinmek için gerekli olan sürecin kullanışlılığını ve netliğini de onaylamıştır.

Etiket elde etmenin önemli prosedürleri hakkında soru sorulduğunda, çoğu katılımcı web sitesinin (Portalın) kullanılabilir olduğunu ifade etmiştir. Etiket alma sürecinin güvenilirliğinin

yanı sıra web sitesinde mevcut bilgilerin en üst sıralarda yer alması gerektiğini de belirtmişlerdir.

Değerlendirme formunun doldurulmasından önce alınan destek portalda yeterli mi?

Ankete göre öğretmenlerin büyük çoğunluğu, değerlendirme formu sunulduktan sistem üzerinden okulların aldığı eylem planında herhangi bir değişiklik yapmayı düşünmediklerini söylemişlerdir.

Eylem planı, üst seviye etiketin verilmesinden önce ele alınması gereken ve daha da geliştirilmesi gereken alanları vurguladığından okulun çevrimiçi güvenliğini arttırmada önemli bir rol oynamaktadır.

Katılımcıların sadece küçük bir yüzdesi Eylem Planının basitleştirilmesi ve daha net hale getirilmesi gerektiğini önermiştir.

Çalışmaya katılanların oldukça yüksek bir yüzdesi, okul personelinin çevrimiçi güvenlik uygulamaları bağlamında daha fazla destek alma ihtiyacını vurgulamıştır. eSafety Etiketi girişiminin, okullarda hareket edebilecek organizasyonlar veya otoritelerle anlaşmalar yaratması ve bu nedenle ulus ötesi eğitim programları yoluyla bir "Kural/Akreditasyon" uygulamasının gerekli olduğunu ortaya koyabilir.

Rapor, eğitimcilerin çoğunluğu okul personeli ve okul topluluğunun çevrimiçi güvenliği içeren birçok konuda eğitmek almaları için okullarında etkinlikler düzenlenmesi gerektiğini ifade etmişlerdir. Ebeveynlerin bilişim araçlarının kullanımı ve okullarda çevrimiçi güvenlik ile ilgili konular hakkında bilgi sahibi olmaları gerektiği ve çevrim içi güvenlik alanında aktif bir şekilde yer almaları gerektiği yine eğitimciler tarafından belirtilmiştir.

AUP nedir?

“Kabul Edilebilir Kullanım Politikası” anlamına gelir. AUP (Acceptable Use Policy), bir web sitesini veya internet servisini kullanmak için uymanız gereken kuralların listesidir. Yazılım lisans sözleşmesine (SLA/Software license agreement) benzer, ancak özellikle internet hizmetleri için kullanılır.

En iyi bilinen, yüksek trafikli web siteleri, hizmet şartları (TOS/Terms of Service) veya Kullanım Şartları (TOU/Terms of Use) olarak da adlandırılabilecek bir AUP içerir. Sık sık, web sitesinin AUP’sine ana sayfanın alt kısmında bir link bulabilirsiniz.

Bulut uygulamaları gibi birçok web hizmeti, çevrimiçi hizmeti kullanmak için bir AUP’ye katılmanızı gerektirir. ISS’ler genellikle, takip etmeniz gereken belirli kuralları belirten her hesap için bir AUP sağlar.

Bir AUP’nin özellikleri sunulan hizmete bağlı olarak değişir. Web sitesi AUP’leri bile web sitesinin amacına ve web sitesinin içeriğine bağlı olarak büyük farklılıklar gösterebilir.

Genel AUP kuralları:

Herhangi bir şekilde yasaları ihlal etmeyin.

Başkalarının haklarını ihlal etmeyin.

Virüsleri veya diğer kötü amaçlı yazılımları dağıtmayın.

Yetkisiz bir alana veya hesaba erişmeye çalışmayın.

Başkalarının telif haklarına ve fikri mülkiyetine saygı gösterin.

Kullanım yönergeleri hakkında bilgi edinin ve ihlalleri bildirin.

AUP, kullanıcı ile çevrimiçi hizmeti sunan şirket arasında bir anlaşma yapar. Bazı kurallar temel kurallardır, bazılarının yasal sonuçları olabilir. Bir AUP’daki bir politikaya uymamanız durumunda, şirket hesabınızı askıya alma, feshetme veya gerekirse yasal işlem yapma hakkına sahiptir. Bu nedenle, kullandığınız İnternet servislerinin AUP’lerini tanımanız akıllıca olacaktır.

AUP ve Okul ilişkisi:

Ankete katılanların önemli bir yüzdesinin Kabul Edilebilir Kullanım Politikası (AUP) belgesi olmadığı ortaya çıkmıştır. AUP, kullanıcıların internete güvenle erişmelerini ve mobil

teknolojilerle etkileşime girmelerini sağlayan bir dizi kullanıcıya rehberlik eden kısa bir belgedir. Bu, eSafety Label + projesinin, Avrupa'daki daha fazla okulda Kabul Edilebilir Kullanım Politikası veya 'Okul Politikası' şablonunun uygulanmasını önerebileceği anlamına gelir.

Ayrıca, anket sonuçları eSafety etiket akreditasyon sürecinin tamamının yalnızca teknik süreç açısından değil, aynı zamanda ilgili çeşitli aktörler arasındaki etkileşimler söz konusu olduğunda çok iyi alındığını ve yüksek kalitede olduğunu göstermektedir. Spesifik olarak, Ulusal Koordinatörlerin rolü, katılımcıların cevaplarının netliği ve hızı ve toplam sürece katma değeri bakımından büyük beğeni toplamıştır.

Raporda vurgulanan bir diğer iyileştirme alanı da olay davası (Vaka incelemesi) deposudur. Anket sonuçları, katılanların çoğunun, çevrimiçi olarak rapor vermenin önemini, topluluk üyeleri arasında iyi uygulama ve bilgi paylaşımı aktarımını tam olarak algılayamadıklarını ortaya çıkarmıştır. Buna bağlı olarak eSafety Label portalının yenilenen versiyonu olaylara ve bunların nasıl sergilendiğine çok daha fazla önem vermektedir.

Son olarak bu rapor, eSafety Label + projesinin, henüz okulu bronz, gümüş veya altın bir etiket kriterlerini karşılamayan eğitimcileri nasıl motive etmesi gerektiğini de vurgulamaktadır.

Bu motivasyon iki farklı yolla gerçekleştirilebilir:

1. İçerik açısından, üç temel eSafety çalışma alanını kapsayan güncel eylem planları ve kontrol listeleri sağlayarak: Altyapı (yani ağ güvenliği), Politika (yani, Kabul Edilebilir Kullanım Politikaları) ve Uygulama (yani, danışmanlık)

2. Pedagojik bir bakış açısına göre, eğitimcilerin birbirlerine liderlik etmelerini, kapsamlı en iyi uygulama çözümlerinin daha da yaygınlaştırmasını sağlayan dinamik bir eSafety Şampiyonu grubu koçluğu oluşturarak.

Okullarının ihtiyaçlarına uygun bir çevrimiçi güvenlik stratejisi oluşturmak isteyen eğitim uzmanlar, "Gelecek için eSafety Şampiyonu Ol" sloganı ile MOOC (Ücretsiz çevrim içi kurs) katılımcıların okullarda uygun eSafety politikalarının önemini düşünmelerine, eSafety risklerini belirlemelerine, okullarının ve öğrencilerinin okullara yönelik bir okul yaklaşımı uygulamasında onlara karşı karşıya gelmelerine ve desteklemelerine yardımcı olacaktır.

"Forum bölümü oldukça özenli kullanılması gereken bir bölümdür. Forum bölümünü inceleyen veya katılmak isteyen birçok yabancı öğretmenin sizin mesajınızı / gönderinizi okuyacakları, inceleyecekleri unutulmamalıdır."

Kullanıcı adı ve şifresi ile eSafety Label portalına erişildikten sonra "Collaborate" (İşbirliği) sekmesi tıklanır.

Bu bölüm eSafety etiket topluluğuna aktif katılımınıza ve çevrimiçi güvenliğe ilişkin görüş ve bilgilerinizi arkadaşlarınızla paylaşmanıza olanak sunar. Bu alanda kendi uzmanlığınızı diğer topluluk üyeleriyle paylaşabilir, düşüncelerinizi ifade edebilir, sorular sorabilir veya başkalarının deneyiminden yararlanabilirsiniz.

Yine "Collaborate" (İşbirliği) ana sayfasında bulunan "Forum highlights" (Forumun özeti) bölümünden "Go to forum" botonu tıklanıp forum bölümüne geçiş yapılır.

Forum genel olarak 4 ana kategoriden oluşmaktadır:

1. eSafety etiketi ve elçiler bölümü

eSafety Label elçileri için hazırlanmış olan bu bölümü ülkenizde bulunan elçilerle iletişim kurmak veya Erasmus+ projesine katılımınızı göstermek için kullanabilirsiniz.

2. eSafety etiketi girişimi bölümü

Değerlendirme sürecinden bahsetmek, ilerlemeniz hakkında fikirlerinizi paylaşmak, eSafety Etiketi üyelerine sorular sormak için bu alanı kullanabilirsiniz.

Alt kategoriler: Akreditasyon süreci, diğer sorular veya tereddütler, portal hakkında sorular ve teknik konular.

3. Tanıtımlar ve genel yorumlar

Bu alanı genel yorumlar, kendinizi tanıtmak veya eSafety Etiketi ile ilgili olmayan konuları tartışmak için kullanabilirsiniz.

Alt kategoriler: Kendinizi tanıtın, Öğretmen buluşma yeri – Felemenkçe, Öğretmen buluşma yeri – Yunanca, Öğretmen buluşma yeri – Portekizce, Öğretmen buluşma yeri – İspanyolca, Öğretmen buluşma yeri – Macarca

4. Çevrimiçi güvenlik tartışmaları

Okulunuzda çevrimiçi güvenlikle ilgili haberleri, tereddüte düştüğünüz durumları, soruları veya durumları paylaşmak için bu alanı kullanabilirsiniz.

Alt kategoriler: Etkinlikler ve kampanyalar, çevrimiçi güvenlik eğilimleri ve yenilikler, çevrimiçi güvenlikle ilgili sorular

Mesaj panoları:

Bu alan forum sayfasının girişinde bulunan sekmeler grubunu içerir. Bunlar:

1. Mesaj panoları ana sayfa

2. Yakın zamanda gönderilenler

3. Gönderilerim

4. Aboneliklerim

5. İstatistik bölümü

Ayrıca “Search” (Araştır) kutucuğundan aradığınız konu başlıklarını hızlı ve kolayca bulabilirsiniz.

Forum bölümünde mesaj yazmak için “Post new thread” (Yeni konu gönder) butonu tıklanır. Açılan yeni sayfada mesaj yazılabilir, istenirse mesaja resim eklenebilir. Son olarak “Save as draft” (Taslak olarak kaydet), “Preview” (Ön izleme), “Publish” (Yayınla), Cancel (İptal) tercihlerinden bir tanesi seçilir.