



**eSafety Label**  
for a safer school

# eSafety Label Hakkında Herşey



# **eSafety Label**

Hakkında Herşey

Burhan SEL

İÇERİK GELİŞTİRME	Burhan SEL
GRAFİK TASARIM	Burhan SEL
EDİTÖR	Turan GÖRE
ISBN	978-605-68191-4-8
BASKI	e-Kitap
YAYIN YILI ve YERİ	ADANA, 2019
VERSİYON	1. Dijital Sürüm
LİSANS	Kitap içeriğindeki tüm materyaller, ticari olmaksızın kaynak gösterilerek kullanılabilir, paylaşılabilir
LİSANS Creative Commons	CC BY-NC
YAZAR İLETİŞİM	burhan.sel@meb.gov.tr

Gelecek neslin mimarı tüm öğretmenlere,  
saygıyla



## ÖNSÖZ

Günümüzde eğitim öğretim çağında bulunan nesil Z kuşağı olarak tanımlanıyor. Bu “Dijital” kuşak diğer tanımlı kuşaklardan daha keskin sınırlarla ayrılırken, eğitimcilerin devinim içindeki bu kuşağı iyi analiz etmesi ve eğitim politikalarının yeni neslin ihtiyaçlarına göre şekillenmesi büyük önem taşıyor.

2000 yılı sonrası doğan ve Z kuşağını oluşturan bu grup sanal iletişim tabanlı alt yapıya sahip, teknolojiyi hızlı şekilde kavrayan, kısa sürede işleri çözüme ulaştırmayı seven, ileri seviye teknolojiyi kullanabilen, giyilebilir teknolojiyi yaşamalarının parçası olarak gören, kısaca hayatı dijital yaşayan bir kitleyi oluşturuyor.

Bu kuşağın gelecekte hayatlarında yoğun olarak yapay zeka ve robot teknolojisinin yer alacağı öngörülüyor. Buluş yöntemi ile öğrenen, meraklı ve üretken olan bu nesil akademik olarak da çok yönlü olmayı tercih ediyor.

Tüm bu öngörü ve bilimsel verilerin sonucunda, her geçen gün önemini arttıran dijital güvenlik kavramı da yetişmekte olan yeni neslin mutlak en önemli ihtiyacı olacaktır. Biz öğretmenlerin eğitim öğretiminden sorumlu olduğumuz kuşağı çok iyi tanıyıp, e-Güvenlik alanındaki beklentilerini, ihtiyaçlarını tespit etmemiz gerekiyor.

Bu noktada eTwinning projelerinde çok önemsenen kişisel verilerin kullanım ilkelere, eSafety (Elektronik güvenlik) kavramı, eSafety Label portalı ve okullar için e-Güvenlik akreditasyonu, her yıl kutlanan güvenli internet günü, ülkemizde imzaladığı e-Güvenlik ile ilgili uluslararası sözleşmeler doğru bir öngörü ve mükemmel bir kurgu ile ortaya çıkmıştır.

Gelecek neslin ihtiyaç ve beklentilerine göre yenilikçi eğitim metotları ve kavramlar ortaya çıkmaya devam etmektedir. e-Güvenlik de gelecek kuşağın en çok ihtiyacı olacak kavramlardan bir tanesidir.

Ayrıca eTwinning okulu kavramının internet güvenliği, e-Güvenlik üzerine kurgulanması; eTwinning portalında yapılan çalışmalarda e-Güvenliğin önemsenmesi; ulusal ve ulus ötesi alanda yapılan projelerde kişisel verilerin korunması kanununa yer veriliyor olması dijital güvenlik kültürünün önemini ön plana çıkarmaktadır.

Ülkemizde de okulların e-Güvenlik alanında politikalarını oluşturdukları ve eylemsel olarak çevrim içi ve çevrim dışı uygulamalarını gerçekleştirdikleri **“e-Güvenlik etiketi hizmetleri değerlendirme ve akreditasyon aracı”** olan eSafety Label portalı gün geçtikçe daha fazla okulun sisteme dahil olması ile büyük bir hızla gelişiyor.

eSafety Label hakkında tüm detayların anlatıldığı bu eğitim çalışmasında 12 eğitim modülü bulunuyor. Bu modüller:

- Modül 1: eSafety Label Nedir?
- Modül 2: Güvenlik Etiketi Basamakları
- Modül 3: eSafety Label Portalı
- Modül 4: eSafety Label Sistemine Kayıt
- Modül 5: Değerlendirme Formu
- Modül 6: Kaynaklar Bölümü
- Modül 7: Vaka İncelemesi Bölümü
- Modül 8: Okul Aksiyon Planı
- Modül 9: eSafety+ Hakkında
- Modül 10: Forum Bölümü
- Modül 11: eTwinning ve eSafety Label
- Modül 12: eTwinning School için eSafety Label

*“Meraklı, yaratıcı, sürekli öğrenen, kılavuzluk yapan, kendini sürekli öz değerlendiren, 21. yy bilgi ve becerilerinden haberdar, teknolojiyi araç olarak kullanmayı bilen, global vatandaşlık kavramını hisseden, öğrencileri kendi kendilerine öğrenmeye doğru yönelten, öğrenen kuşakları iyi tanıyan ve analiz eden, işbirlikçi çalışmayı önemseyen ve geleceğe dokunmanın yolunun düşünce gücü özgür, hayal gücü geniş, değerler kavramını özümsemiş bireylerden geçtiğinin farkında olan, bilgiyi paylaşmayı seven bir eğitimci ya kesinlikle bir eTwinner’dır veya eTwinner olmalıdır.”*

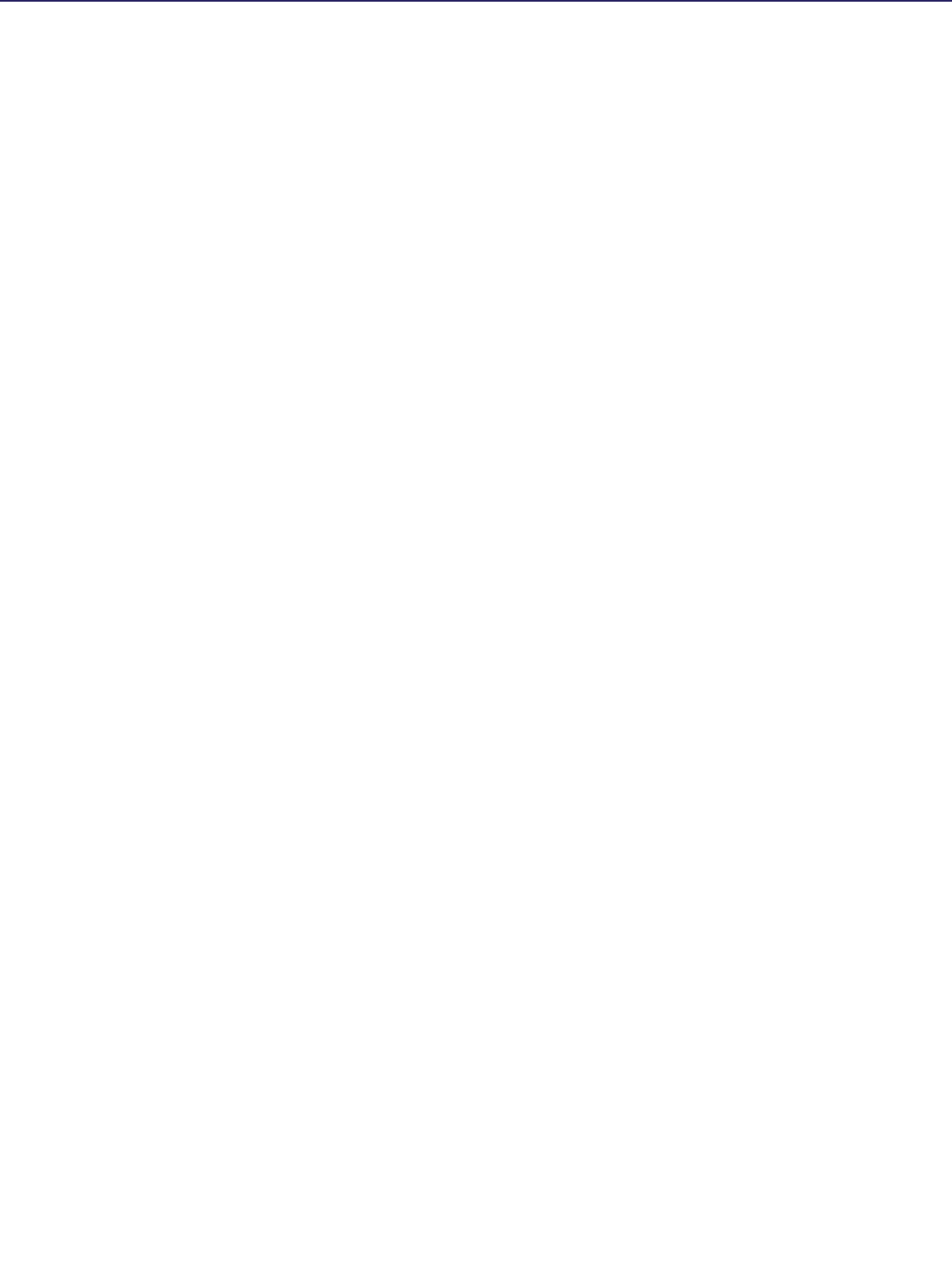
eSafety Label platformunun anlatıldığı bu çalışmanın tüm öğretmenlere yararlı olması dileğiyle.

Burhan SEL  
2019, Adana

## İÇİNDEKİLER

Önsöz.....	V
İçindekiler.....	VII
Modül 1: eSafety Label Nedir?.....	9
Modül 2: Güvenlik Etiketinin Basamakları.....	12
Modül 3: eSafety Label Portalı.....	24
Modül 4: eSafety Label Sistemine Kayıt.....	30
Modül 5: Değerlendirme Formu.....	36
Modül 6: Kaynaklar Bölümü.....	55
Modül 7: Vaka İncelemesi Bölümü.....	24
Modül 8: Okul Aksiyon Planı.....	30
Modül 9: eSafety+ Hakkında.....	36
Modül 10: Forum Bölümü.....	55
Modül 11: eTwinning ve eSafety Label.....	55
Modül 12: eTwinning School için eSafety Label.....	57
Kaynakça.....	59





### eSafety Label Nedir?

Her geçen gün önemi daha iyi kavranan e-Güvenlik kavramı artık dijital ortamda bireysel güvenlikten öteye giderek, kurumların ve ülkelerin politikalarına dahil olmuştur.

Çevrim içi olarak eSafety Label'in resmi adresi olan [www.esafetylebel.eu](http://www.esafetylebel.eu) üzerinden ulaşılan modül, okullar için Avrupa çapında bir akreditasyon ve destek hizmetidir. eSafety Label, eğitim ve öğrenim deneyiminin bir parçası olarak çevrim içi teknolojiye güvenli erişim için güvenli ve zenginleştirici bir ortam sağlamayı hedeflemektedir.

eSafety Label web sitesi, öğretmenler, okul müdürleri ve bilişim yöneticileri için önemli bir politika oluşturma merkezidir. Okulların kendi çevrim içi güvenliklerini değerlendirdikleri, iyileştirdikleri ve güçlendirdikleri hareket eylem yapısıdır. Okulların kendi çevrim içi güvenlik altyapısını, politikalarını ve uygulamalarını ulusal ve uluslararası standartlara göre gözden geçirmek eSafety Label sayesinde mümkün olmaktadır.



eSafety Label Topluluğu, 38 ülkeden yaklaşık 4.000 öğretmen ve Eğitim Bakanlıkları, üniversiteler, Güvenli İnternet Merkezleri gibi irtibat noktalarını bir araya getiren geniş bir ağıdır.

Sürekli gelişen bir kavram olarak e-Güvenlik veya “Çevrim içi güvenlik”, kullanıcıların çevrim içi olarak sahip oldukları becerileri, davranışları, eriştikleri içerikleri ve çalıştıkları çevrim içi içeriği kapsamaktadır.

Teknoloji kullanımının yönetilmesine yardımcı olmak isteyen ve okulların bu anda artan ihtiyaçlarını kabul eden önde gelen teknoloji şirketleri, eğitim bakanlıkları ve Avrupa Okul Ağı güçlerini birleştirip çok paydaşlı bir organizasyon kurmuşlardır. ESafety Label inisiyatifi, 2012 yılında bu ortak taahhütten doğmuştur.



Avrupa Okul Ağı ve eSafety Label arasındaki konsorsiyum Avusturya, Estonya ve İspanya'daki Eğitim Bakanlıkları ve eğitim kurumları aracılığıyla eylemsel olarak desteklenmiş ve daha fazla Avrupa ülkesine yayılmıştır.



Ülkemizde de okulların e-Güvenlik alanında politikalarını oluşturdukları ve eylemsel olarak çevrim içi ve çevrim dışı uygulamalarını gerçekleştirdikleri **“e-Güvenlik etiketi hizmetleri değerlendirme ve akreditasyon aracı”** eSafety Label portalı gün geçtikçe daha fazla okulun sisteme dahil olması ile büyük bir hızla gelişiyor.

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

European SchoolNet (Avrupa okul ağı) kapsamında yürütülmekte olan eTwinning, Scientix, Europeana, Safer Internet Day gibi Avrupadaki öğretmenleri de içine alan geniş kapsamlı çalışmalarda e-Güvenlik kavramı oldukça önemsenmektedir.



### Güvenlik Etiket Basamakları

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 portalda yapılan anket çalışmasındaki 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 bölümü, 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 portalda 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 alışverişi yapmak üzere mutlaka bir araya gelmelidir. Beyin fırtınası ile okulun e-Güvenlik alanındaki 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 formundaki 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.

**“Etiket değerlendirme süreci, değerlendirme formunun puanına, kaynak teslimine ve topluluğa aktif katılıma bağlıdır.”**





**Demir / Etiket yok:** 22 puandan az puan alırsanız, başvurunuz Demir olarak tanımlanır. Okuldaki e-Güvenlik alanında yapmanız gereken çalışmalarını 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.



**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 çevrim içi 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.



**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 çevrim içi güvenlik politikasının, uygulamasının ve altyapısının bir Gümüş Etiket hak edip etmediğine karar verecektir.





**Altın Etiket:** Değerlendirme formunda en az 55 puan alan okullar içindir. Bu etiket için Topluluk'taki kaynaklar, olay vakaları ve etkinlikleri, çevrim içi güvenliğin tüm alanlarında yoğun çalışılmış uygulamalar sergilenmeli ve çevrim içi 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.



## eSafety Label Portalı

eSafety Label portalını 2 aşamada incelemek gerekir.

İlk aşama sisteme kayıt olmaksızın tüm ziyaretçilere açık olan sekmeler ve bölümler, diğeri ise sisteme kayıt olduktan sonra açılan sekmeler ve bölümlerdir.

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.)

### About:

“Hakkında” sekmesinde eSafety Label’ın, güvenli ve zenginleştirici bir ortam sağlamayı hedefleyen, öğretim ve öğrenme deneyiminin bir parçası olarak çevrim içi teknolojiye güvenli erişim için okullar için Avrupa çapında bir akreditasyon ve destek hizmeti olduğundan bahsedilmektedir.

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

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

### Online Safety:

“Çevrim içi güvenlik” sekmesinde eSafety Etiketini ile okullara, öğrencilere, ebeveynlere ve personellere çevrim içi 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 çevrim içi güvenlik yönlerinin okul eylem planları ile sunulduğu anlatılmaktadır.

## Modül 3: eSafety Label Portalı

Alt yapı bölümünde internetin çok çeşitli avantajlar ve fırsatlar sunduğu, ancak içinde risklerin de 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.

Politikalar bölümünde okul politikalarının düzenli olarak gözden geçirilmesi gerektiğinin farkına varılmasının önemli olduğu, özellikle çevrim içi 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.

Okulunuzun 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.

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.

### eSafety Label:

“eSafety Etiket” 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.

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.

Okulunuzun çevrim içi güvenlik seviyesine ve değerlendirme sürecinde değerlendirilen diğer faktörlere bağlı olarak, aşağıdaki etiketlerden birini alabileceğiniz ifade edilmektedir. Bunlar:

**Demir:** Temel çevrim içi güvenlik seviyesi (Etiket tanımlanmaz)

**Bronz:** Çevrim içi güvenlik konusunda asgari farkındalık

**Gümüş:** Çevrim içi güvenliğe daha gelişmiş bir yaklaşım

**Altın:** Çevrim içi güvenliğin tüm alanlarında ve çevrimiçi güvenliğin eğitiminde üstün uygulama

### 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.

### 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 çevrim içi güvenlik konularında okulların akreditasyonunun birçok kuruluş tarafından desteklendiği bilgilerine ve ilgili endüstri ortakların ve ulusal ortakların tanıtımına yer verilmiştir.

Ayrıca sayfada ortak olmak isteyen kuruluşlar için iletişim bağlantısı verilmiştir.

### eSafety Champions:

“e-Güvenlik şampiyonları” sekmesinde ücretsiz çevrim içi kurslara katılıp bilgi ve tecrübenizi arttırabileceğinizin anlatıldığı sayfada, bu çevrim içi kursların eSafety politikalarının oluşturulmasında, eSafety risklerini belirlenmesinde, okulların öğrencilere yönelik yaklaşımlarının oluşmasında fayda sağlayacağı ifade edilmektedir.

## Modül 3: eSafety Label Portalı

e-Güvenlik şampiyonları çevrim içi 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.

### 2. Aşama: Sisteme kayıtlı üyelere açık bölümler



Sisteme kayıt olduktan sonra ziyaretçilerin görebildiği tüm sayfalara ek olarak yeni sekmeler açılır.

#### 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.

Topluluğun tüm araçlarını keşfetmenizi, okulunuzun çevrim içi güvenliğini artırmak için neler yapabileceğinizi ve belgelendirmek için bir eSafety Etiketini nasıl alabileceğiniz bilgilerinin bulunduğu sayfadır. Kullanıcı profili ve okul hesabına bu sayfadan ulaşılmaktadır.

#### Prepare:

“Hazırlık” sekmesi öz değerlendirme süreci hazırlıklarının yapıldığı bölümdür. Uluslararası öğretmenler topluluğuna, yöneticilere ve çevrim içi güvenlik uzmanlarının olduğu eSafety portalına katılarak okulunuzun çevrim içi güvenliğini artırma yolunda ilk adımı atmış olduğunuz anlatılmaktadır.

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.

Ve 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.

### **Collaborate:**

“İşbirliği” sekmesinde eSafety Etiket Topluluğuna katılmak, çevrim içi güvenliğe ilişkin görüş ve bilgilerinizi arkadaşlarınızla paylaşmanıza olanak tanıdığından, bu alanda uzmanlığınızı ve düşüncelerinizi diğer topluluk üyeleri ile paylaşabileceğinizden, sorular sorup veya başkalarının deneyiminden yararlanabileceğinizden bahsedilmektedir.

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

### **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.

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.

## Modül 3: eSafety Label Portalı

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.

### Resources:

“Kaynaklar” sekmesinde çevrim içi güvenlik kaynakları, modern teknolojinin ve çevrim içi 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.

Kaynakların yüklenmesi, diğer öğretmenlerin daha güvenli bir çevrim içi ortam oluşturmaya yardımcı olacak ve okulunuzun eSafety Etiket akreditasyonu için ekstra puan kazanacağınız açıklanmaktadır.

Sayfada “Bir kaynak yükle” bölümü de bulunmaktadır.

### 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 çevrim içi 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 oluşturmaya yardımcı olmanız istenmektedir.

Okulunuzun eSafety Etiket akreditasyonu için vakalar bölümünün önem taşıdığından söz edilmektedir.

Sayfada “Bir vaka bildir” bölümü de bulunmaktadır.

## eSafety Label Sistemine Kayıt

Ana ekran 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.

### EUN ID Login

Username

Password

[Login](#)

[Create an account](#)

[Forgot EUN ID login/password?](#)



## Modül 4: eSafety Label Sistemine Kayıt

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. Ekranaya 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.

**Register**

First name (First name)

First name

Family name

Family name

Email

Email

Password

Password

Confirm password

Confirm password

Security check

I am not a robot

reCAPTCHA

Submit

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.



## Modül 4: eSafety Label Sistemine Kayıt

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 özgeçmiş 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.

The screenshot shows a web form titled "About yourself". The form contains several input fields and dropdown menus. The fields are: "First name" (with a dropdown menu showing "Panna sándor"), "Family name" (with a dropdown menu showing "Gyimes"), "Country" (with a dropdown menu showing "Magyarország"), "Mother tongue" (with a dropdown menu showing "Magyar"), "Other spoken languages" (with a dropdown menu showing "Angol", "Francia", "Német", "Spanyol", "Svéd", "Tudok más nyelven is"), "Describe yourself" (a large text area), and "Website" (a text field). At the bottom of the form, there is a red "Submit" button. The form is set against a light blue background with a subtle pattern.

“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.

## Modül 4: eSafety Label Sistemine Kayıt

Eğer kullanıcının okulu açılan seçeneklerde gözükyorsa 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.

The following matching organisations were found

Adana Dehaşatin İskokul	Adana Real Artç Yeri	This is my organisation
Adana Zihni Akademi Lisesi	İstanbul Mahallesi 2002. sok. 010401	This is my organisation
Beyoğlu İsmaili Primary school	Bilezikade Mevludin Değbey Cadde. NO:33 ÇEYHANADANA 01000	This is my organisation
Çelebi Mehmet İlkokulu	Cemalpaşa mhi. Garipapa cad. 5109 01140	This is my organisation

Click on the button below to add your organisation to the list.

Yeni okul eklemek için aşağıdaki form adım adım doldurulur:

### About your organisation

First name (with or without surname)  
Please select a value

Address  
Please enter an address (street and number)

City  
Please select a value

Post code  
Please enter a post code

Country  
Please select a value

Region  
Please select a value

Phone  
Please enter a phone number

Number of seats  
Please enter a value

Minimum age of pupils  
Please select a value

Maximum age of pupils  
Please select a value

Telephone  
Please enter a telephone number (with or without extension)

Email  
Please enter an email address (with or without extension)

Fax  
Please enter a fax number (with or without extension)

ASSET  
Please select a value

The screenshot shows a registration form for the eSafety Label system. It features a grid of checkboxes for selecting subjects, a dropdown menu for 'Country', a text box for 'Description', a dropdown menu for 'Area', and a 'Submit' button. The subjects listed are:
 

- Arts
- Chemistry
- Early Childhood Education
- Educational Administration
- Business Studies
- Geography
- Home Economics
- IT
- Music
- Physical Education
- Pre-school Education
- Religion
- Special Needs Education
- Business
- Computer
- Education
- Economic Education
- Foreign Language
- Health Education
- Information/ICT
- Mathematics
- Natural Science
- English
- Civics Education
- School/Community Relationships
- Learning
- History
- Digital Language
- Assessment
- Ethics
- Gender
- Money
- Language and Identity
- Health Education
- Philosophy
- Politics
- Social Studies

“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.

## Modül 4: eSafety Label Sistemine Kayıt

“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.

Yeni okul ekleme işlemi tamamlandıktan sonra değerlendirme formu bölümü aktif hale gelmektedir.

## Değerlendirme Formu

Kapasite geliştirme eSafety etiketini edinmede ilk adım olsa da, tüm süreç boyunca devam etmekte ve okulların akranlar ve uzmanlarla bilgi alışverişinde buldukları, 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 ise bir dizi sorudan oluşmaktadır.

Değerlendirme formu sonucunda okulun toplamda alacağı puan oldukça önemlidir. Bunun yanı sıra okulun kaynaklar, olay durumları ve topluluk üzerindeki faaliyetleri yoluyla eSafety topluluğuna katkısı dikkate alınacak, bir uzman faaliyetinizi gözden geçirecek ve Demir, Bronz, Gümüş veya Altın etiketlerinden birini okul akreditasyon sürecinde kuruma tanımlayacaktır.



## Modül 5: Değerlendirme Formu

### 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.

## Modül 5: Değerlendirme Formu

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.

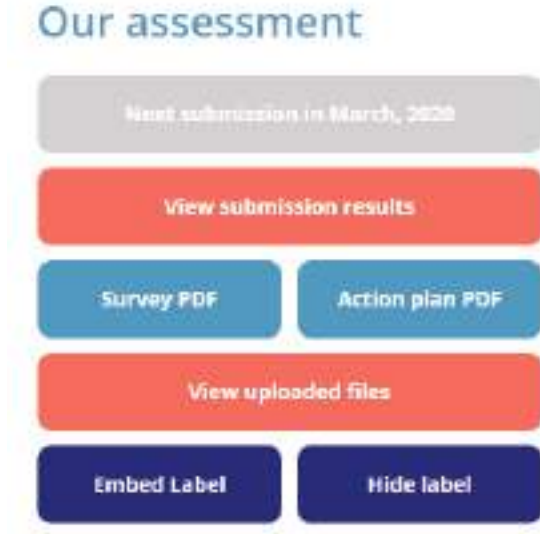
Okul SWOT analizlerinde, stratejik planlarında, öğretmenler kurul toplantılarında e-Güvenlik ile ilgili güncel politikalar işlenmeli ve gündeme alınmalıdır. Okul öğretmen ve öğrencilerinin e-Güvenlik konusunda duyarlı ve bilinçli olmaları, bilgilerini okul yönetimi kılavuzluğunda sürekli güncel tutmaları 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.



Form değerlendirme detaylarına Submission detail bölümünden erişilebilir:

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

### Dip Not:

Son olarak profil bölümünden okul adı tıkladığı 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](http://storage.eun.org/esafety-label-medal/Bronze_2017_11_en_b7249.png)” şeklinde yazılmalıdır. (Tırnak işaretleri olmaksızın)

Okul web sayfasına eSafety Label etiketini eklemek ve bağlantı vermek için fare imleç etiketin üzerinde iken sağ tıklanıp, resmi farklı kaydet seçeneği ile resim kayıt edilebilmektedir.

### Kaynaklar Bölümü

Kaynaklar bölümü (Our resources), okulda e-Güvenlik alanında yapılan örnek uygulamaların sisteme yüklendiği bölümdür.

Bu noktada yapılan genel bir hata, eğitimcilerin “Forum” bölümünde örnek uygulamalarını paylaşımları kaynaklar bölümüne yükleme yapmamalarıdır.

Eğitimciler, okullarının hem görünürlüğünü arttıracak hem de eSafety Label etiketini geliştirme anlamında ek puanlar (Bonus puanlar) kazandıracak kaynaklar bölümüne mutlaka örnek uygulamalar yüklemelidirler.

Bu bölüm, sisteme kayıtlı olan eğitimcilerin diğer meslektaşlarının e-Güvenlik alanında yaptıkları örnek uygulamaları görmeleri açısından önemli bir alandır.

Kaynaklar formu doldurulurken dikkat edilmesi gereken noktalar, formda açılan tüm sorulara cevap vermek, en fazla 3-4 adet anahtar kelimeyi sisteme girmek, sisteme yüklenen bir resim ise telif hakkı konusunda bilgi vermek ve formun altında bulunan form gönderme onay butonunun işaretlenmesi gerekliliğidir.



Our resources bölümüne ulaşmak için ana sayfada yer alan **Community** sekmesi tıklanır. Açılan sayfada **My Organisation** butonu tıklanır.





### Vaka İncelemesi Bölümü

Vaka incelemesi (Our cases), 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.



Our cases bölümüne ulaşmak için ana sayfada yer alan **Community** sekmesi tıklanır. Açılan sayfada **My Organisation** butonu tıklanır.



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

Vaka incelemesi (Our cases) formu içerisinde birçok açılır menü şeklinde seçim butonları bulunmaktadır.

Form doldurulurken vaka incelemesine uygun olan ifadelerin yer aldığı butonlar mutlaka doğru işaretlenmelidir.

## Form Bölümleri:

Yeni bir vaka oluştur

Yeni bir vaka oluştur

Değiştir

Yeni bir vaka oluştur

Yeni bir vaka oluştur

Tarih seçmek istemiyorsanız "Data range" seçilmelidir

Tür:

Konu başlığı:

Languaj:

Hangi dil seçeneği ile sorular isteme yaptığınız:

Yüklenmiş:

Açılır pencereden sorular tiplerinden bir tanesini seçilir  
(Siber zorbalık, uygunsuz iletişimçerik, gözetimlik ihlali, cinsel taciz veya diğer)

Seviyeler:

Açılır pencereden okul türünüz seçilir

Yakınlaşım seviyeleri:

Açılır pencereden dış katılımcıları seçilir  
(Öğretmen, öğrenci, okul yönetimi, polis gibi)

Okul türü/okul seviyesi:

Açılır pencereden okuyucu yer seçilir  
(Evde, okul dışı ders sırasında, okulda ders dışında, okul dışında, diğer gibi)

Sınıflar:

Okulu dışlayarak anlatılır

Yararlı kayıtlar:

Yararlı kayıtlar

Diğer açıklamalar:

Diğer açıklamalar istediğiniz yorumlar

Bu vaka için formun, soruların içerik ve formel geçerliliğini kontrol edip bu formu işleme tabii tuttuğumuzu ifade eder. Soruların içeriğini kontrol ettiğimizi garanti ederiz. Soruların içeriğini kontrol ettiğimizi garanti ederiz. Soruların içeriğini kontrol ettiğimizi garanti ederiz.

Kayıt Wazgeç

Bu formu göndererek, verilen bilgilerin doğru olduğunu onaylarsınız.

Bu vakanın eSafety portalı "Okul Vaka Tiplerinde ve eSafety Dikkat Ökölünde" ve/veya çalışmaları ve / veya bu uygulama materyallerini geliştirmek amacıyla kişisel bilgileri kullanılarak değerlendirilmesi kabul ediyorsunuz.

Bu QR çubuğunun anarşini hale getirilmesini, okuyucuları ve kendinizin bilgilerin güll tutulacağını biliyorsunuz.

Son olarak mutlaka kullanım sözleşmesi onaylanmalıdır.



### Okul Aksiyon Planı

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

Planda okulun güçlü ve zayıf yönlerinin 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 Etiketisi – Eylem Planı

“... okulu için ... tarafından sunulan eylem planı – tarih @ saat”

“Doldurulmuş “Değerlendirme Formunu” eSafety Etiketisi 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 değildirler. Bununla birlikte, her yaştaki öğrencilere bir eğitim yaklaşımı ve esneklik kazandırmak da güvenli ve sorumlu çevrim içi 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.

## Modül 8: Okul Aksiyon Planı

### 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 açısından 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](http://www.inhope.org)) yasadışı içerik bildirmeyi ve şüphelendiğiniz durumları bildirmeyi unutmayın. Türkiye için [ihbarweb.org.tr](http://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 çevrim içi 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.

### Online Okul Varlığı

- Okul Politikanızın tüm alanları kapsadığını göstermek için okulda fotoğraf ve videoların izinsiz çekilmesi ve yayınlanması hakkındaki politikanızı öncelikle hayata geçirin.
- Okulunuzun çevrim içi itibarını kontrol edecek bir okul yöneticisinin veya öğretmenin 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 çevrim içi güvenlik sorunlarıyla başa çıkmak için destek sunmanız önemlidir. Öğrencilere okul dışında çevrim içi teknolojiyi kullanmalarını hakkında mutlaka eğitim verilmelidir.
- Öğrencilerinizin çevrim içi alışkanlıklarıyla ilgili bilgilerini eSafety Etiketini topluluğu aracılığıyla diğer okullarla paylaşabilirsiniz. Örneğin, öğrencilerin çevrim içi 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 konumdur. Okul Politikanızı geliştirmeye ve düzenli olarak gözden geçirmeye katkıda bulunmak için okuldaki diğer personeller toplantılara davet edilmelidir.
- Okulunuzdaki öğrencilerin aktif olarak eSafety mentorları 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 yüklemeye 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 geliştirmedeğinizi 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+ Hakkında

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 çevrim içi 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 çevrim içi 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

[www.esafetylevel.eu/esafety-champions](http://www.esafetylevel.eu/esafety-champions) adresini ziyaret ediniz.”



## Modül 9: eSafety+ Hakkında

Sonuç olarak bu arařtırmalar, okulların ihtiya ve güçlerini çevrim ii güvenlik aısından geliřtirmeleri için řu adımların atılması gerektiđi ortaya ıkarmıřtır:

1. eSafety Etiketini akreditasyon sürecini öğretmenler ve diđer okul personeli için kolaylařtırılmalı,
2. eSafety Label topluluđu tarafından sađlanan bilgilerin kapasitenin geliřtirilmesinde daha iyi hale getirilmesi için alıřılmalı,
3. Okul personeli için eSafety adımlarının anlatıldıđı rehber geliřtirmek.

### **Raporda ortaya ıkan ana ıktılar ve öneriler:**

Genel olarak, bu arařtırmanın dayandıđı anketin sonuçları ok olumlu olmuřtur. Katılımcıların ođunluđunun deđerlendirme formu ile ilgili bir iyileřtirmenin gerekli olmadığını düřündükleri ortaya ıkmıřtır. Bu, bir eSafety etiketini edinmek için gerekli olan sürecin kullanılabilirliđini ve netliđini de onaylamıřtır.

Etiket elde etmenin önemli prosedürleri hakkında soru sorulduđunda, ođu katılımcı web sitesinin (Portalın) kullanılabilir olduđunu ifade etmiřtir. Etiket alma sürecinin güvenilirliđinin yanı sıra web sitesinde mevcut bilgilerin en üst sıralarda yer alması gerektiđini de belirtmiřlerdir.

### **Deđerlendirme formunun doldurulmasından önce alınan destek portalda yeterli mi?**

Ankete göre öğretmenlerin büyük ođunluđu, deđerlendirme formu sunulduktan sistem üzerinden okulların aldıđı eylem planında herhangi bir deđerlik yapmayı düřünmediklerini söylemiřlerdir.

Eylem planı, üst seviye etiketin verilmesinden önce ele alınması gereken ve daha da geliřtirilmesi gereken alanları vurguladıđından okulun çevrim ii güvenliđini arttırmada önemli bir rol oynamaktadır.

Katılımcıların sadece küçük bir yüzdesi “Eylem Planı”nın basitleřtirilmesi ve daha net hale getirilmesi gerektiđini önermiřtir.

Çalışmaya katılanların oldukça yüksek bir yüzdesi, okul personelinin çevrim içi güvenlik uygulamaları bağlamında daha fazla destek alma ihtiyacını vurgulamıştır. eSafety Etiketleri 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 çevrim içi güvenliği içeren birçok konuda eğitmek almaları için okullarında etkinlikler düzenlenmesi gerektiğini ifade etmişlerdir. Ebeveynlerin bilişim araçlarının kullanımı ve okullarda çevrim içi 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 adlandırılabilir bir AUP içerir. Sık sık, web sitesinin AUP'sine ana sayfanın alt kısmında bir link bulabilirsiniz.

Bulut uygulamaları gibi birçok web hizmeti, çevrim içi 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.

## Modül 9: eSafety+ Hakkında

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 çevrim içi 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 inceleme-si) deposudur. Anket sonuçları, katılanların çoğunun, çevrim içi 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, **3 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.

Detayları anlatılan rapora

<http://etwinningonline.eba.gov.tr/wp-content/uploads/2019/09/I01-Research-report.pdf> adresinden ulaşabilirsiniz.

### **Bir sonraki eSafety Şampiyonu MOOC (Ücretsiz çevrim içi kurs) için hemen kaydolun**

Okullarının ihtiyaçlarına uygun bir çevrim içi 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.

### **eSafety Label + Champion materyalleri yayınlandı**

Kaçırmanız durumunda, öğretmenlerin öğretmenler için yarattığı bir dizi yeni çevrim içi güvenlik kaynağı 2019 Güvenli İnternet Günü eSafety Label web sitesinde yayınlandı.

ESafety Label + Champions, öğretmenler için veri koruma, medya okuryazarlığı veya siber zorbalık gibi temalara değinen bir dizi yeni çevrim içi güvenlik kaynağı hazırladı ve yayınladı. Öğretmenler için öğretmenler tarafından oluşturulan bu eğitim kaynakları, ders planları için öneriler, öğrencilerle kullanılacak materyaller, öz değerlendirme formları ve rehberlik sayfalarını içermektedir.

## Forum Bölümü

“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 çevrim içi 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” (Forum özeti) bölümünden “Go to forum” butonu 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.

CATEGORY	CATEGORIES	THIRAGE	POSTS
<b>eSafety Label + Ambassadors</b> If you are an Ambassador, use this area to engage with fellow Ambassadors or users, and to showcase your involvement in the Erasmus+ project.	6	13	31
<b>eSafety Label initiative</b> Please use this area to talk about the assessment process, to talk about your progress, to ask questions to fellow eSafety Label members. <b>Subcategories:</b> Activities/Workshops, Other questions or advice, Policy questions and technical advice	1	31	57
<b>International and general concerns</b> Use this area for general comments, to reproduce general and recurring issues not related to eSafety Label. <b>Subcategories:</b> eSafety awareness, Teacher meeting (date - EU), Teacher meeting (date - Czech), Teacher meeting (date - Portugal), Teacher meeting (date - Spanish, More...	6	71	130
<b>Diverse safety discussions</b> Use this area to share online safety related news, adults' questions or situations (grade encouraged), to give advice. <b>Subcategories:</b> Events and Conferences, Child safety (news and how-tos), Questions about online safety	1	21	56

## 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 tanıtmak, Öğretmen buluşma yeri - Felemenkçe, Öğretmen buluşma yeri - Yunanca, Öğretmen buluşma yeri - Portekizce, Öğretmen buluşma yeri - İspanyolca, Öğretmen buluşma yeri - Macarca.

## 4. Çevrim içi güvenlik tartışmaları

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

Alt kategoriler: Etkinlikler ve kampanyalar, çevrim içi güvenlik eğilimleri ve yenilikler, çevrim içi güvenlikle ilgili sorular.

## Mesaj panoları:



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

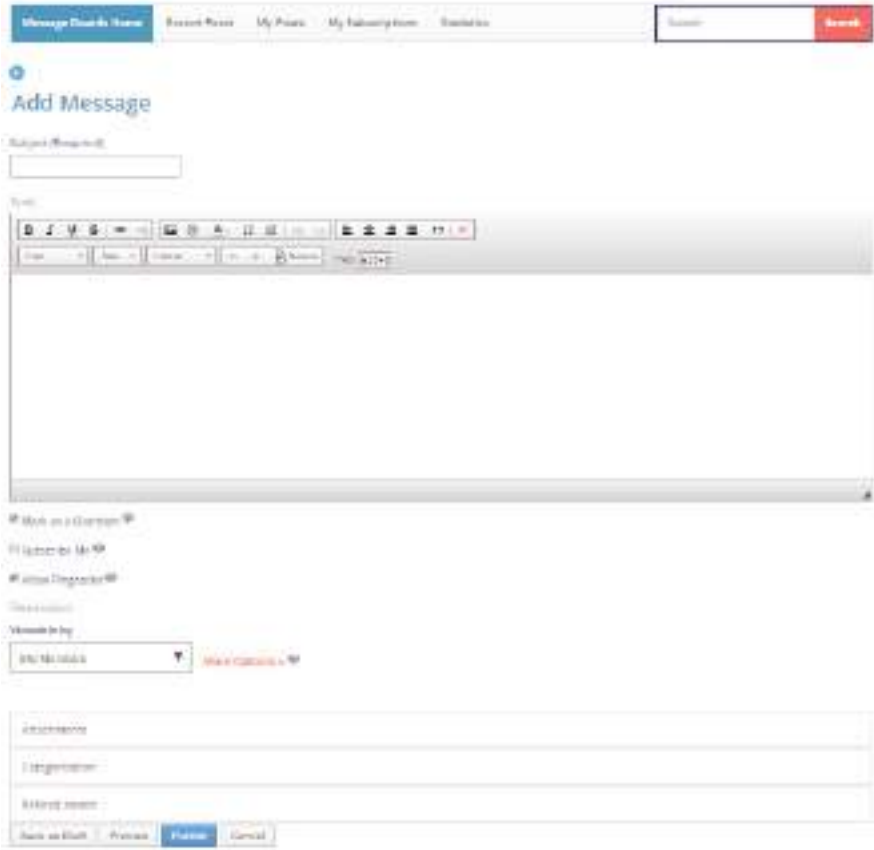
1. Mesaj panoları ana sayfa
2. Yakın zamanda gönderilenler
3. Gönderilerim
4. Aboneliklerim
5. İstatistik bölümü

## Modül 10: Forum Bölümü

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

Mesaj panosunun kullanılması oldukça kolaydır. Forum bölümünde mesaj yazmak için “Post new thread” (Yeni konu gönder) butonu tıklanır. Bu aşamada aşağıdaki mesaj panosu açılacaktır:

### Message Boards



The screenshot shows the 'Add Message' form in a forum interface. At the top, there is a navigation bar with links for 'Message Boards Home', 'Recent Posts', 'My Posts', 'My Following users', and 'Statistics'. A search bar is located on the right side of the navigation bar. Below the navigation bar, the main heading is 'Add Message'. The form includes a 'Subject (Required)' field, a 'Body' field with a rich text editor toolbar, and a 'Who to notify' section with checkboxes for 'Mark as a Favorite', 'Notify by Email', and 'Allow Pingbacks'. There is also a 'Visable to log' dropdown menu. At the bottom, there are fields for 'Attachments', 'Tags', and 'Keywords', along with 'Save as Draft', 'Preview', 'Publish', and 'Cancel' buttons.

Açılan sayfada Add Message (Mesaj ekle) bölümü çıkacaktır. “Subject” (Konu başlığı) bölümü mutlaka doldurulmalıdır. “Body” (Mesaj içeriği) bölümüne mesaj yazılır, istenirse mesaja ilgili sekmeler aracılığı ile resim de eklenebilir.

Son olarak “Save as draft” (Taslak olarak kaydet), “Preview” (Ön izleme), “Publish” (Yayınla), Cancel (İptal) tercihlerinden bir tanesi seçilir.

### eTwinning ve eSafety Label

GDPR (General Data Protection Regulation) nedir?

eTwinning ve eSafety Label arasındaki bağlantıyı daha iyi anlayabilmek için GDPR kavramını gözden geçirmek gerekmektedir.

Avrupa Birliği “Genel Veri Koruma Yönetmeliği” (GDPR), tüm Avrupa genelinde AB vatandaşlarını korumaya yönelik uyumlu bir dizi veri gizliliği yasası hazırlamak için geliştirilmiştir. Bu düzenleme, 95/46/EC sayılı veri koruma direktifi'nin yerini almıştır. Ancak bu veri koruma düzenlemesi önceki veri koruma direktifinden ciddi olarak farklılık göstermektedir. Bunlar şu şekilde özetlenebilir:

**1. Daha geniş yetki alanı:** Yeni düzenleme ile Genel Veri Koruma Yönetmeliği, Avrupa Birliği sınırları içerisinde yaşayan herhangi bir kişinin kişisel verilerini işleyen tüm şirketler için, şirketin kendi konumu fark etmeksizin geçerli olacaktır.

**2. Cezalar:** Genel Veri Koruma Yönetmeliği ile uyumlu olmayan denetleyiciler ve işleyiciler dahil tüm kurum ve kuruluşlar, yıllık küresel cirolarının %4'üne veya 20 milyon avroya (hangisi büyükse) varan miktarlarda ceza alabilir.

**3. Onay:** Kişisel verilerin kullanımına dair onay, net ve kolayca anlaşılır bir şekilde istenmeli ve diğer konulardan ayırt edilebilmelidir. Buna ek olarak, onayın geri alınması da verilmesi kadar kolay olmalıdır.

**4: İhlal Bildirimleri:** Yeni düzenleme ile kişisel verilerin ihlal bildirimleri zorunlu olacaktır ve kurum veya kuruluşun ihlalin farkına varmasını takip eden 72 saat içinde tamamlanması gerekecektir.

**5: Gizlilik:** Genel Veri Koruma Yönetmeliği, veri koruma işlevinin sistemler tasarlanırken baştan dahil edilmesini, sonradan ekleme yoluyla uygulanmamasını şart kılar.

Tüm AB vatandaşlarının veri gizliliğini koruyan ve güçlendiren; bölge genelinde kuruluşların veri gizliliğine yaklaşma şeklini yeniden şekillendiren; Avrupa genelinde veri gizliliği yasalarını birbiri ile uyumlu hale getiren GDPR (Genel Veri Koruma Yönetmeliği) bireyler, kurumlar ve şirketler için çok önemli sorumluluklar / yükümlülükler getirmektedir.



## Modül 11: eTwinning ve eSafety Label

Bu noktada European School Net platformunun önemli projelerinden bir tanesi olan eTwinning platformunda çevrim içi projeler yapan tüm eğitimciler “Genel Veri Koruma Yönetmeliği” çerçevesinde proje yönetimlerini revize etmeye başlamışlardır.

Avrupa Birliği’ne bağlı olan ülkelerde gizlilik kavramı yıllarca öncesinde mevcuttu, ancak Genel Veri Koruma Yönetmeliği ile bu durum yasal bir zorunluluk haline gelmiştir.

eTwinning portalı, bilindiği gibi öğretmenleri ortak paydalarda proje tabanlı öğrenme için aynı çatı altında buluşturmanın ötesinde öğretmen yeterliliklerinin gelişimini de önemsemektedir.

Öğretmenlerin çevrim içi öğrenme kurslarına katılımları, portal üzerinden hazırladıkları projelerin niteliği ve niceliği sonucu kalite etiketi almaları, çevrimiçi etkinlikler hazırlamaları portalda oldukça önemsenmektedir. Yine portal da hazırlanan projelerde görevli bireylerin Genel Veri Koruma Yönetmeliği çerçevesinde kişisel hak ve mahremiyetleri **eTwinning ve eSafety (e-Güvenlik)** arasında mutlak güçlü bir bağlantı olması gerektiğini ortaya koymaktadır.

Özellikle dijital kültür ile beraber gelen “Dijital ayak izi”, bireylerin sanal dünyada bıraktıkları izler olarak adlandırılmaktadır. Eğitimcilerin, ebeveylelerin izinleri olmaksızın etkinlik ve/veya projede görevli küçük yaş grubu öğrencilerin dijital içeriklerini çevrim içi veya çevrim dışı paylaşmamaları hem etik değerler hem de veri koruma kanunları gereği bir zorunluluktur.

Hazırlanan veya uygulanmakta olan eTwinning projeleri sürecinde ve proje bitiminde başvuru kalite etiketi sürecinde çevrim içi güvenlik kurallarına uyum ve kişisel verilerin korunması oldukça önemsenmektedir. Bu noktada eSafety Label okul eylem planı, eTwinning projelerinde aktif görev alan eğitimci ve öğrenciler için e-Güvenlik konusunda önemli bir kılavuzluk görevi üstlenmektedir.

eSafety Label etiketi, sadece okulların veri koruma ve yönetme ile ilgili akrediyasyon sürecini değil, aynı zamanda okuldaki eğitimcilerin ve öğrencilerin e-Güvenlik alanında atacakları adımları da tanımlar.

### eTwinning School için eSafety Label



eTwinning Okulu uygulaması, portal üzerinden projeler yapan öğretmenlerin buldukları okuldaki diğer meslektaşlarına örnek olabilmelerine, yenilikçi eğitim anlayışında olan öğretmenlerin sayılarının artmasına, eTwinning okulu seçilen okulun diğer okullara örnek/önder olabilmelerine; okul yöneticilerinin evrilen ve gelişen eğitim sistemini anlatabilmelerine, okullarının ulusal ve ulus ötesi farkındalık kazanmalarına olanak sağlıyor. Bunun yanı sıra gelecekte Erasmus+ eylem hareketleri ile şekillenecek okul hareketliliklerine ve daha kaliteli projeler oluşturulmasına da zemin hazırlıyor.

eTwinning portalında yeni bir adım olan ve örnek okul seçimi olarak da adlandırılan “eTwinning Okulu”; e-Güvenlik politikalarının uygulandığı, eTwinning çevrim içi projelerinin aktif olarak yürütüldüğü, öğretmenlerinin ulus ötesi öğrenme etkinliklerine katılıp eğitim aldığı, okul öğretmenleri tarafından hazırlanan eTwinning projelerinin kalite etiketleri ile ödüllendirildiği bir okulun öğretmeni olmak “Yenilikçi öğrenen ve öğreten” ilkesi ile hareket eden öğretmenler ve yöneticiler için ayrıcalıklar sağlıyor.

Bu noktada eTwinning Okulu sürecinde oldukça önemsenen eSafety (e-Güvenlik) kavramı gelecek kuşağın en çok ihtiyacı olacak kavramlardan bir tanesi olarak ön plana çıkıyor. eTwinning Okulu kavramının internet güvenliği ve e-Güvenlik üzerine kurgulanması, okulların e-Güvenlik politikalarının ve uygulamalarının olma gerekliliği, işbirlikçi öğretimi ve eTwinning portalında yapılan çalışmaların yaygınlaştırılmasını önemsemesi e-Güvenlik kavramının eTwinning platformu için ne kadar önemli olduğunu ortaya koymaktadır.

eTwinning Okulu ünvanı, bir okulun geneli için geçerlidir. Okul yöneticileri ve öğretmenlerini içine alan, e-Güvenlik ile ilgili okulların politika oluşturmasını bekleyen bir anlayıştır. Buna bağlı olarak e-Güvenlik akreditasyon aracı olan eSafety Label, okulların e-Güvenlik politikalarını belirlemelerinde kurumlara profesyonel kılavuzluk sağlamaktadır.

e-Güvenlik uygulamalarının okul politikalarından biri olması ve okul yönetim ekibinin/öğretmenlerinin bu politikaların yürütücüleri olmaları eTwinning okulu sürecinde önemsenmektedir.

## Modül 12: eTwinning School için eSafety Label

eTwinning okulu başvuru basamaklarında birçok bölüm e-Güvenlik konusunda okulun yeterliliklerini sorgulamakta, öğretmenlerin e-Güvenlik alanında yaptıkları çalışmaları kanıtlamalarını istemektedir.

Başvuru kılavuzu Bölüm 1.1 de eTwinning platformunda ve okulda e-Güvenlik farkındalığının geliştirilmesine yönelik yapılan çalışmalar istenmektedir. Bu noktada, eğer okul politikası kısmen e-Güvenlikle ilgili çalışma yapıyor veya hiç yapmıyorsa bu aşamada okulun bu yeterliliklerini geliştirmesi gerektiğine dair olumsuz geri bildirim alınabilir. Bu bölümde ikinci soruda taşınabilir cihaz ve cep telefonlarının okulda kullanımı ile ilgili okulun bir politikaya sahip olup olmadığı konusunda; üçüncü soruda öğrencilerin, okul personelinin ve velilerin fotoğraflarının çekilmesi, onların fotoğraf çekmesi ve yayınlamalarının denetimi ile ilgili bilgi istenmektedir. Bu noktada eSafety Label okul eylem planı başvuru formu doldurulurken çok güçlü bir dayanak ve kılavuz olacaktır.

Başvuru kılavuzu Bölüm 1.2 de e-Güvenliğin uygulamada nasıl aktif hayata geçirildiğine dair bilgi istenmektedir. Örneğin beşinci soruda öğrenci velilerine e-Güvenlik ile ilgili yapılan bilgilendirme çalışmaları hakkında bilgi; altıncı soruda okul öğretmenlerinin e-Güvenlik konularıyla ilgili aldıkları eğitimler hakkında; yedinci soruda okulda güvenli internet günü kutlamaları hakkında bilgi istenmektedir. Bu noktada yine eSafety Label okul eylem planı başvuru formu doldurulurken çok güçlü bir dayanak ve kılavuz olacaktır.

e-Güvenlik kavramının okul politikasının ayrılmaz bir parçası olduğunu kanıtlamak için, e-Güvenlik uygulamalarının okul politikalarından biri olduğundan ve okul öğretmenlerinin müfredat derslerinde konuya atıfta bulduklarından söz edilebilir. Aday okulun eSafety Label etiketi aldığından ve e-Güvenlik eylem planı olduğundan, bu güvenlik politikaları hakkında okul öğretmenlerinin bilgilendirildiğinden bahsedilebilir.

Varsa sınıf ve okuldaki bilgisayarların virüs ve uygunsuz içeriklere karşı yazılım korumalarının olduğundan, okul öğretmen ve öğrencilerine dijital bağımlılık konusunda bilgilendirme etkinliklerinin yapıldığından ve bunun sürekli tekrarlandığından söz edilebilir.

eTwinning portalı kullanılması sırasında projede çalışacak öğrencilerin video ve fotoğraflarının sosyal medya ve twinspace ortamında paylaşımına dair velilerinden resmi izin belgesi alındığı da belirtilebilir.

## Kaynakça

### Kitaplar:

ALTUN, Anzilha; SEL, Burhan, eTwinning Okulu Başvuru Kılavuzu, 2018, Adana  
The Teaching Profession in Europe, 2015, European Commission

### İnternet erişimi:

[www.esafetylabel.eu](http://www.esafetylabel.eu)  
[www.eun.org](http://www.eun.org)  
[www.eugdpr.org](http://www.eugdpr.org)  
[www.etwinning.net](http://www.etwinning.net)  
[etwinning.meb.gov.tr](http://etwinning.meb.gov.tr)  
[www.schooleducationgateway.eu](http://www.schooleducationgateway.eu)  
[www.betterinternetforkids.eu](http://www.betterinternetforkids.eu)  
[www.btk.gov.tr](http://www.btk.gov.tr)  
[www.etwinningonline.eba.gov.tr](http://www.etwinningonline.eba.gov.tr)

- Modül 1: eSafety Label Nedir?
- Modül 2: Güvenlik Etiketleri Basamakları
- Modül 3: eSafety Label Portalı
- Modül 4: eSafety Label Sistemine Kayıt
- Modül 5: Değerlendirme Formu
- Modül 6: Kaynaklar Bölümü
- Modül 7: Vaka İncelemesi Bölümü
- Modül 8: Okul Aksiyon Planı
- Modül 9: eSafety+ Hakkında
- Modül 10: Forum Bölümü
- Modül 11: eTwinning ve eSafety Label
- Modül 12: eTwinning School için eSafety Label

“Her geçen gün önemi daha iyi kavranan e-Güvenlik kavramı artık dijital ortamda bireysel güvenlikten öteye giderek, kurumların ve ülkelerin politikalarına dahil olmuştur.

Çevrim içi olarak eSafety Label'in resmi adresi olan [www.esafetylevel.eu](http://www.esafetylevel.eu) üzerinden ulaşılan modül, okullar için Avrupa çapında bir akreditasyon ve destek hizmetidir. eSafety Label, eğitim ve öğrenim deneyiminin bir parçası olarak çevrim içi teknolojiye güvenli erişim için güvenli ve zenginleştirici bir ortam sağlamayı hedeflemektedir.

eSafety Label web sitesi, öğretmenler, okul müdürleri ve bilişim yöneticileri için önemli bir politika oluşturma merkezidir. Okulların kendi çevrim içi güvenliklerini değerlendirdikleri, iyileştirdikleri ve güçlendirdikleri hareket eylem yapısıdır. Okulların kendi çevrim içi güvenlik altyapısını, politikalarını ve uygulamalarını ulusal ve uluslararası standartlara göre gözden geçirmek eSafety Label sayesinde mümkün olmaktadır.”

