

e-Safety Label Eylem Planı

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

Altyapı

Teknik güvenlik

- Okul sisteminiz bir güvenlik duvarı tarafından korunuyor. Güvenlik duvarının sağlanması ve yönetiminin gerektiğinde ve gerektiğinde düzenli olarak gözden geçirildiğinden ve güncellendiğinden emin olun.
- Bilişim hizmetlerinin artık kullanılmaması durumunda düzenli olarak gözden geçirilmesi, güncellenmesi ve kaldırılması iyi bir uygulamadır.
- Acil olarak okul ağında korunması gereken cihazlar için virüs koruması sağlamanız gerekir, çünkü bunların yalnızca bazıları korunmaktadır. Yalnızca virüslü bir cihaz okulun tüm ağını kirletebilir ve belirli virüs türleri yasadışı içeriği sunucunuza bile kaydedebilir. Hem okul politikanızda hem de Kabul Edilebilir Kullanım Politikanızda virüs korumasına ilişkin bir paragraf içermeli ve personelin ve öğrencilerin okul kurallarını titizlikle uyguladığından emin olmalısınız. Cihazlarınızı kötü amaçlı yazılımlara karşı koruma hakkında bilgi için

www.esafetylabel.eu/group/teacher/protecting-devices-against-malware adresini ziyaret edin.

Öğrenci ve personel teknolojiye erişim

- Personel ve öğrencilerin okuldan sonra USB bellek çubuklarını kullanmalarına izin verilmesi, ilgili tüm personelin ne zaman güvenli bir şekilde kullanılabileceğini bilmek için yeterli eğitim almasını gerektirecektir. Bu böyle mi? Sisteminizi, personelinize ve öğrencilerinize izin verirken güvende tutmak için, Kabul Edilebilir Kullanım Politikanıza temel kuralları da eklemeniz gerekir. Tüm güvenlik hususlarını ele aldığınızdan emin olmak için **www.esafetylabel.eu/group/teacher/removable-devices** adresindeki çıkarılabilir cihazların kullanımı hakkındaki gerçeklere bakın.
- Okulumuzdaki bilgisayar laboratuvarlarında kolayca rezervasyon yaptırmanız iyidir. Diğer dijital cihazları derslere dahil etme seçeneğini göz önünde bulundurun; bunları kullanarak yeni medya ile ilgilenen öğrenciler için en iyi uygulamayı sağlayın. Güvenlik konularının da tartışıldığından emin olun.

Veri koruması

- Okulunuz için belirli okul kayıtlarının nasıl depolandığını, arşivlendiğini ve bertaraf edildiğini gösteren bir saklama planı vardır. Bu çok iyi. Planın takip edildiğinden emin olun ve Veri Koruma Yasası ve diğer ilgili mevzuatla ilgili olmasını sağlamak için düzenli olarak gözden geçirin. Daha fazla bilgi için ilgili bilgi formuna bakınız.
- Öğrenme ve yönetim ortamlarınızı ayrı tutma konusunda iyi bir politikanız var. Politikalarınızı incelemeye devam ederken bu ortamları yönetme konusunda eğitim almış personelin güncel

olmasını sağlamak iyidir. Politikanızı okul profilinize yükleyerek diğer eSafety Etiket kullanıcılarıyla paylaşın.

- Okulunuzun cihazları, özellikle taşınabilir cihazları korumanın önemi konusunda eğitim materyalleri sağlaması iyidir. Lütfen bunları içeride başkalarıyla paylaşmayı düşünün. Ayrıca, malzemelerinizin en son teknolojiye uygun olmasını sağlamak için düzenli olarak incelenmelerini sağlayın.

Yazılım lisansı

- Okulunuzdaki tüm yazılımların yasal olarak lisanslı olduğundan ve lisansların kopyalarının merkezi olarak tutulduğundan emin olmanız gerekir. Ayrıca, BT sisteminizi kimin desteklediğini, yazılımın sistem güvenliğinden ödün vermeyeceğini kontrol etmeniz gerekir. Okulunuz yazılım alımı için net bir politika geliştirmelidir ve bu süreci mümkün olan her yerde merkezileştirmek iyi bir uygulamadır.

BT Yönetimi

- Okul bilgisayarlarında kurulu olan yeni yazılımların kullanımı konusunda eğitim ve / veya rehberlik etmeniz iyi bir uygulamadır. Bu, okul üyelerinin yeni özelliklerden yararlanmalarını, aynı zamanda gerektiğinde güvenlik ve veri koruma konularının farkında olmalarını sağlar.

Politika

Kabul Edilebilir Kullanım Politikası (AUP)

- Okul topluluğunun tüm üyeleri için Kabul Edilebilir Kullanım Politikanız olması iyi bir şey. AUP'un hala amaç için uygun olduğundan emin olmak için düzenli olarak gözden geçirin; AUP'nizin yeterince kapsamlı olmasını sağlamak için, bilgilendirme sayfasına ve www.esafetylevel.eu/group/teacher/acceptable-usepolicy adresindeki Kabul Edilebilir Kullanım Politikası hakkındaki kontrol listesine bakın.
- Amaca uygun olduğundan ve okulda tutarlı bir şekilde uygulandığından emin olmak için Cep Telefonu Politikasını düzenli olarak gözden geçirin. Okulda cep telefonu kullanımı (www.esafetylevel.eu/group/teacher/mobile-phones) ve Okul Politikası (www.esafetylevel.eu/group/teacher/school-policy) hakkındaki ayrıntılı bilgiler yararlı bilgiler sağlayacaktır.
- Okul politikalarının okulunuzda yıllık olarak gözden geçirilmesi iyidir. Bunları etkileyebilecek değişiklikler yapıldığında da güncellenmelerini sağlayın. Tüm personel politikanın içeriğinin farkında olmalıdır.
- Okulunuzda politika konuları düzenli olarak tartışılmaktadır. Bu, personelin ve öğrencilerin onlardan haberdar olmalarını sağladığı için iyi bir uygulamadır. Öğrenciler ve personel farkındalıklarını doğrulamak için ilgili belgeleri de imzalamak zorunda mı?

Raporlama ve Olay İşleme

- Okul Politikanızın, öğretmenler, öğrencilerin bilerek veya istemeden yanlışlıkla yasadışı veya hakaret edici materyale çevrimiçi olarak öğrettikleri ogreticiday.de/en web sitesi (tinyurl.com/9j86v84) tarafından belirlenen rehberliğe girerek, bildikleri veya hatta istemeden yasadışı veya rahatsız edici materyale eriştiği zamanlarla ilgili tüm bilgileri içerdiğini kontrol edin. Okulunuzda bu tür olaylar ortaya çıkarsa, eSafety Etiket Olayı işleme formunu isimsiz olarak doldurduğunuzdan emin olun (www.esafetylevel.eu/group/teacher/incident

Başka okulların tecrübelerinden yararlanabilmesi için).

- Okul dışında meydana gelen çevrimiçi olaylar' politikasını daha açık hale getirin ve bunun Okul Politikası ve Kabul Edilebilir Kullanım Politikası ile herkese açıkça iletilmesini sağlayın. Okulların birbirlerinin stratejilerini paylaşmalarını ve öğrenmelerini sağladığı için Olay işleme formunda (www.esafetylevel.eu/group/teacher/incidenthandling) olayları anonim olarak belgelemeyi unutmayın.
- Okul politikasının, akıllı telefonlar gibi potansiyel olarak güvenli olmayan cihazlara sahip riskler hakkında bilgi içermesi ve bu referansın yapılması iyi bir uygulamadır. Okul politikanızı, Okul alanımdan da erişilebilen yükleme kanıtı aracıyla paylaşmayı düşünün.

Öğrenci uygulaması / davranış

- Elektronik iletişim kurallarını Kabul Edilebilir Kullanım Politikanızda tanımladınız ve bu, diğer okullar için iyi bir uygulama örneğidir. Diğer okulların deneyiminden faydalanabilmesi için, öğrenciler için elektronik iletişim kuralları hakkında bir öğretici oluşturabilir ve bunları Okul alanım üzerinden okul profilinize yükleyebilir misiniz?

Online okul varlığı

- Uygun olmayan yorum bulunmadığından emin olmak için okulun çevrimiçi sosyal medya sitelerindeki varlığını düzenli olarak kontrol edin. Siteyi / sayfayı güncel tutmak için bir süreç oluşturun ve iyi uygulama yönergelerinin bulunduğundan emin olmak için daha fazla bilgi için Sosyal Ağlardaki Okullar konulu bilgi notuna

(www.esafetylevel.eu/group/teacher/social-networks) bakın. takip edildi. Profilin ne kadar yararlı olduğu konusunda paydaşlardan geri bildirim alın.

Practice

Management of eSafety

- Okulunuzda, öğretmenler kendi öğrencilerinin çevrimiçi etkinliklerinden sorumludur. Öğrencilerinizin ve okul ağlarının güvenliğini sağlamak için yapılması gereken birçok ağ güvenliği ve kullanıcı gizliliği, denetimi ve prosedürel aracı kontrolü ve dengesi vardır ve bunlar Okul Politikanızda belirtilmelidir. **www.esafetylevel.eu/group/teacher/school-policy** adresindeki Okul Politikası hakkındaki gerçek sayfamıza bakın.
- Bunun olabildiğince verimli ve sık gerçekleşmesini sağlamak için, okul müdürünüzün okuldaki eSafety yönetimine bakması için bir bireysel personel atamasını tavsiye ederiz. Bu kişi, Okul Politikanızda yer alan tüm konuların sınıfta öğrencilerle olduğu gibi diğer öğretmenlerle de tartışıldığını ve onlara bakıldığını görmekle sorumlu olacaktır.
- Her personelin, öğrencinin ve velinin, çevrimiçi hak ve sorumluluklarının farkında olmasını sağlamak için, Kabul Edilebilir Kullanım Politikası (**www.esafetylevel.eu/group/teacher/acceptable-use-policy**) hakkındaki bilgi notuna bakınız.
- ESafety için atanan vali veya yönetim kurulu üyesinin düzenli eğitim alma ve aynı zamanda meslektaşlarının eSafety konularının farkında olmalarını sağlama fırsatına sahip olduğundan emin olun. Okul Politikanızı geliştirmeye ve düzenli olarak gözden geçirmeye idari organınızı dahil edin. Okul Politikaları **www.esafetylevel.eu/group/teacher/school-policy** hakkındaki gerçek sayfamıza bakın.
- ESafety'den sorumlu bir personelin olması iyi bir şey. Tüm paydaş gruplarından üyelerden oluşan bir eSafety komitesine sahip olmanın faydalı olup olmadığını düşünün. Bu kişinin Okul Politikanızı geliştirirken ve düzenli olarak gözden geçirirken yer aldığından emin olun. Yalnızca

bilgilendirilmemeli, ayrıca www.esafetylevel.eu/group/teacher/incident-handling adresinde bir olay meydana geldiğinde Olay işleme formunu doldurmalıdır.

Müfredatta eSafety

- Okulunuzda siber zorbalığın, müfredatta genç yaşta öğrencilerle tartışılması iyi bir uygulamadır.
- Çocuk koruma politikanız dahilinde cinselliğe özel bir atıfta bulunmanız iyi bir şey çünkü bu, birçok genç insanın uğraşmak zorunda olduğu büyüyen bir konudur. Bu konuda öğrenciler için uygun bir eğitim sağladığınızdan emin olmanız da önemlidir.
- Okulunuzdaki tüm yıl gruplarındaki tüm öğrencilerin eSafety hakkında bilgilendirilmesi iyi bir uygulamadır. Sürekli değişen ihtiyaçları karşıladığından emin olmak için müfredatın düzenli olarak gözden geçirilmesi önemini sürdürmektedir. Bu tür bir müfredat inceleme süreciniz varsa, bunu okul profilinizde yayınlayabilmeniz diğer okullara yardımcı olacaktır. Yükleme için okul alanına gidin.

Müfredat dışı etkinlikler

- İstendiğinde, müfredat dışı zaman dışında öğrencilerinize eSafety desteği sağlamanız iyidir. Tüm öğrencilere çevrimiçi güvenlik sorunlarıyla başa çıkmak için destek sunmayı düşünün. Öğrencilerin Facebook mahremiyetini ayarlamalarına yardımcı olmak için bir “cerrahi” yapılması yararlı olabilir. ESafetyLabelportalı bunun için faydalı kaynaklar sağlar: Öğrencilerin www’deki okul dışında çevrimiçi teknolojiyi kullanma hakkındaki gerçeklere bakın. esafetylevel.eu/group/teacher/socialmedia-pupils.

Destek kaynakları

- Öğrencilere güven öğretmeni görevi gören eSafety konularında bilgili bir personeliniz olması harika.
- Tüm personelin eSafety için bir sorumluluğu olmalıdır. Okul danışmanları, hemşireler vb. Bu konularda tavsiye ve rehberlik sağlayacak şekilde yerleştirilir ve Okul Politikanızı geliştirmeye ve düzenli olarak gözden geçirmeye katkıda bulunmak için davet edilmelidir. Bu personel için eğitim sağlamanın uygun olup olmadığını düşünün.

Personel eğitimi

- Okulunuzda personel üyeleri arasındaki bilgi alışverişi teşvik edilir. Bu, tüm okula faydalıdır. Okulum aracılığıyla da erişilebilen yükleme kanıtı aracı aracılığıyla eSafety konularında PowerPoints, belgeler veya benzer bilgi alışverişi yükleyin.
- Gönderdiğiniz değerlendirme formu büyük bir soru havuzundan oluşturulmuştur. Ayrıca ankette belirtilmeyen alanlarda eSafety’yi geliştirip geliştirmediğinizi bilmek bizim için yararlıdır. Bu tür değişikliklerin kanıtlarını, eSafetyPortalının Okul alanım bölümüne Yükleme kanıtı aracılığıyla yükleyebilirsiniz. Unutma, Değerlendirme Formunun doldurulması Akreditasyon Sürecinin sadece bir kısmıdır, çünkü kanıtların yüklenmesi, Forum aracılığıyla başkalarıyla takaslarınız ve sağlanan şablondaki olayları bildirmeniz de dikkate alınır.