**BURDUR SAKARYA İLKOKULU GÜVENLİ İNTERNET KULLANIMI EYLEM PLANI**

**ALTYAPI**

**TEKNİK GÜVENLİK**:

\*Bilişim hizmetlerinin kullanılmaması durumunda düzenli olarak gözden geçirilmesi, güncellenmesi ve kaldırılması doğru bir uygulamadır.

\*Okul sisteminiz bir güvenlik duvarı tarafından korunuyor. Güvenlik duvarının sağlanması ve yönetiminin düzenli olarak gözden geçirildiğinden ve güncellendiğinden emin olun.

\*Okul cihazlarınızın virüs korumalı olması çok iyi. Hem okul politikanızın hem de Kabul edilebilir Kullanım Politikanızın virüs korumasına ilişkin bir paragraf içerdiğinden emin olun ve personelin ve öğrencilerin okul yönergelerine titizlikle uymalarını sağlayın. Cihazınızı kötü amaçlı yazılımlara karşı koruma hakkında bilgi için: www.esafetylabel.eu/group/community/protecting-your -devices-against-malware adresini ziyaret edin.

**ÖĞRENCİ VE PERSONELİN TEKNOLOJİYE ERİŞİMİ:**

\*Personel ve öğrenciler okul ağında kendi cihazlarını kullandıkları için Kabuledilebilir Kullanım Politikanızın düzenli olarak okuldaki tüm üyeler tarafından gözden geçirildiğinden ve uyarlandığından emin olun. Bu her akademik yılın başında öğrencilerle görüşülmeli.

\*Politikayı teknoloji yerine davranışa dayandırın. Ziyaretçiler okul ağını kullanmadan önce Kabuledilebilir Kullanım Politikasını okumalı ve imzalamalıdır.

\*Personel ve öğrencilerin okulda USB bellek çubuklarını kullanmalarına izin verilmesi ilgili tüm personelin ne zaman güvenli bir şekilde kullanabileceklerini bilmek için yeterli eğitimi almasını gerektirecektir. Bu böyle mi? Sisteminizi personelinize ve öğrencilerinize izin verirken güvende tutmak için Kabuledilebilir Kullanım Politikanıza temel kuralları da eklemeniz gerekir. Tüm güvenlik hususlarını ele aldığınızdan emin olmak için [www.esafetylabel.eu/group/community/use-of-removable-devices](http://www.esafetylabel.eu/group/community/use-of-removable-devices) adresindeki çıkarılabilir cihazların kullanımı hakkındaki bilgi formuna bakınız.

**VERİ KORUMASI:**

\*Öğrenci bilgilerini şifreleme ve güvenli bir şekilde depolamada iyi bir politikaya sahipsiniz. Tüm yeni personelin veri işleme ve şifreleme yöntemlerinin farkında olduğundan emin olun. Okulunuzun veri denetleyicisi olarak görev yapan bir iletişim noktası var. Okul profilinize şifreleme sistemiyle hassas bilgileri koruma hakkında kılavuzlar yükleyin böylece diğer okullar deneyimlerinizden yararlanabilecektir.

\*Okulunuzun cihazları özellikle taşınabilir cihazları korumanın önemi konusunda eğitim materyalleri sağlaması iyidir. Lütfen bunları içeriden başkalarıyla paylaşmayı düşünün. Ayrıca materyallerinizin en son teknolojiye uygun olmasını sağlamak için düzenli olarak incelendiklerinden emin olun.

**YAZILIM LİSANSI:**

\*Tüm yeni personelin yeni yazılımın kurulumu için sahip olduğunuz etkin süreçler hakkında bilgilendirildiğinden emin olmanız önemlidir. Bu şu anlama geliyor ki sistemlerinizin güvenliği korunabilir ve personel, öğretme ve öğrenmeye yardımcı olacak yeni yazılım uygulamalarını deneyebilir.

**POLİTİKA**

**KABULEDİLEBİLİR KULLANIM POLİTİKASI:**

\*E-güvenliğin birçok okul politikasının ayrılmaz bir parçası olması mükemmeldir. Tüm personel öğretme yoluyla bundan bahsediyor mu? İyi uygulama örneklerine bakın ve bunları personel ve öğrencilerle paylaşın. Bu iyi uygulamayı vurgulamak için kısa bir sorun üretin ve diğer okullara ilham olması için okul alanım üzerinden e- güvenlik portalındaki profilinize yükleyin.

**RAPORLAMA VE OLAY İŞLEME:**

\*Tüm personel yasadışı olabilecek materyallerle ilgili prosedürleri iyi biliyor mu? Bu gibi durumlarda tüm sorumluluğu üstlenecek yetkili bir kişi var mı? Okul politikasında tüm personele ; Kabuledilebilir kullanım Politikasında personel ve öğrenciye prosedürün açıkça iletilmesi gerekir.

\*Yasadışı içerikleri Ulusal INHOPE hattına bildirmeyi unutmayın.([www.inhope.org](http://www.inhope.org))

\*Okul merkezli meydana gelen siberzorbalığı kaydetmek iyi bir uygulama çünkü siz ve diğerlerinin gelecekte kullanabilmesi için Avrupa’daki okullardan başarılı olay işleme uygulamaları için bir veri tabanı oluşturmaya katkıda bulunuyorsunuz. Öğrencilerinizin Kabuledilebilir Kullanım Politikasında siberzorbalığa karşı yönergeler imzaladığından emin olunuz.

**PERSONEL POLİTİKASI:**

\*Okul politikasının akıllı telefonlar gibi potansiyel olarak güvenli olmayan cihazlarla ilgili riskler hakkında bilgi içermesi iyi bir uygulamadır. Kanıt aracı yükleyerek okul alanımda okul politikanızı paylaşmayı düşünün.

**ÖĞRENCİ UYGULAMASI/DAVRANIŞ:**

\*Öğrencilerin hayatlarında olup bitenlere dayalı müfredatta ve müfredat dışı e- güvenlik konusunu tartışırken okul etkinliklerini şekillendirme olanağına sahip olması iyidir.

\*Okulunuzun öğrenci davranışları için olumlu ve olumsuz sonuçlara dair okul çapında bir yaklaşımı var. Bu iyi bir uygulama. Lütfen politikanızı e -güvenlik portalında okul alanımda paylaşın böylece diğer okullar da öğrenebilirler.

\*Elektronik iletişim yönergelerini Kabuledilebilir Kullanım Politikanızda tanımladınız ve diğer okullar için bu iyi bir uygulama örneğidir. Öğrenciler için elektronik iletişim yönergeleri hakkında bir eğitim oluşturabilir misiniz ve okul alanım üzerinden okul profilinize yükleyebilir misiniz böylece diğer okullar deneyimlerinizden yararlanabilir.

**ÇEVRİMİÇİ OKUL VARLIĞI:**

\*Öğrencilerin okulun çevrimiçi varlığı hakkında geribildirim verebilmesi iyi. Tamamen öğrenciler tarafından yönetilen bir alan oluşturmayı düşünün. Bu medya okuryazarlığı ve ilgili konular hakkında öğrenmek için büyük bir fırsattır. Ayrıca bir akran destek ağı kurmaya yardımcı olur.

\*Uygun olmayan yorumlar bulunmadığından emin olmak için sosyal medya sitelerinde okulunuzun çevrimiçi varlığının içeriğini düzenli olarak kontrol edin. Siteyi/sayfayı güncel tutmak için bir süreç oluşturun ve iyi uygulama yönergelerinin takip edildiğinden emin olmak için daha fazla bilgiyi sosyal ağlardaki okullarla ilgili bilgi formundan kontrol edin.(www.esafetylabel.eu/group/community/schools-on-social-networks) Profilin ne kadar yararlı olduğu konusunda paydaşlardan geri bildirim alın.

\*Okul politikanızın tüm alanları kapsadığını görmek için okulda fotoğraf ve video çekme ve yayınlama hakkındaki bilgi formunu kontrol edin sonra okul politikanızdaki bu bölümü okul alanım üzerinden profil sayfanıza yükleyin böylece diğer okullar sizin iyi uygulamanızdan yararlanabilirler.

**UYGULAMA**

**E-GÜVENLİK YÖNETİMİ:**

\*Gerekli tüm ağ güvenliği ve kullanıcı gizliliği kontrollerinin yürürlükte olmasını sağlamak için net bir sorumluluk atamasına ek olarak okulların düzenli aralıklarla denetim ve prosedür kontrollerine sahip olması da gereklidir. Bunlarsız bir okul kendini savunmasız bırakacaktır. (www.esafetylabel.eu/group/community/school-policy)

\*Sizin okulunuzda olduğu gibi genel bir lider olması gerekse de okuldaki herkesin günlük mesleki görevlerinde kullandıkları hassas bilgilerin güvenliğini sağlamak için ortak bir sorumluluğu vardır. Veri işlemeye doğrudan dahil olmayan personel bile risk ve tehditler ve sorunların nasıl en aza indirileceği konusunda bilgilendirilmelidir. Kabuledilebilir Kullanım Politikasındaki bilgi formunu kullanın . ([www.esafetylabel.eu/group/community/acceptable-use-policy-aup-](http://www.esafetylabel.eu/group/community/acceptable-use-policy-aup-))

\*Güvenlik için atanan kurul üyesinin düzenli eğitim alma fırsatına sahip olduğundan ve meslektaşlarının güvenlik sorunlarından haberdar olduğundan emin olun. Yönetim biriminizi geliştirme ve düzenli olarak gözden geçirme sürecine dahil edin. ([www.esafetylabel.eu/group/community/school-policy](http://www.esafetylabel.eu/group/community/school-policy))

**MÜFREDATTA E GÜVENLİK:**

\*Çevrimiçi eylemlerin sonuçlarının tüm öğrencilerle tartışılması iyidir. Sözleşme koşullarını tam anlamak için şartlar ve koşulların okunması gerekir. Bu ayrıca veri gizliliğini ilgilendirir. Diğer önemli konu da telif hakkı ihlalidir. Kullandığınız materyalleri kanıt aracı olarak okul alanım üzerinden paylaşın.

\*Ortaya çıkan sorunlarla başa çıkabilen bir e güvenlik müfredatı sağlayabilmeniz övgüye değerdir. Yeni kaynakları kullanılabilir hale getirildikçe kullanmaya devam edin.

\*Okulunuzda sosyal medya kullanımının sonuçları ve sorumlulukları hakkında öğrencilerin küçük yaşta eğitilmesi iyidir. Lütfen okul alanım üzerinden erişilebilen kanıt aracıyla yüklenen herhangi bir kaynağı paylaşın.

**EK MÜFREDAT ETKİNLİKLERİ:**

\*E-güvenlik konusunda öğrenciler arasında akran danışmanlığını nasıl düzenlersiniz? Görüşlerinizi e- güvenlik etiketi forumunda paylaşın böylelikle diğer okullar deneyimlerinizden yararlanabilir ve benzer bir yaklaşım kurabilirler.

\*Müfredat süresi dışında ne tür ek güvenlik desteğinden yararlanacaklarını görmek için öğrencilerden geribildirim toplayın. Bunların bir kısmını akranlarına iletmeye dahil olabilirler mi? Bunları yapmalarına yardımcı olabilecek kaynakları bulmak için e- güvenlik kaynaklar bölümünü kontrol edin. Okul dışında çevrimiçi teknoloji kullanımı için [www.esafetylabel.eu/group/community/pupils-use-of-online-technology-outside-school](http://www.esafetylabel.eu/group/community/pupils-use-of-online-technology-outside-school) bakabilirsiniz.

**DESTEK KAYNAKLARI:**

\*Okulunuzda öğrencilerin e güvenlik danışmanı olmaya aktif olarak teşvik edilmesi harika. Bu ağı güçlendirmeye yönelik yaklaşımınızı forum ya da okul profil sayfası aracılığıyla e-güvenlik etiket sitelerindeki diğer öğretmenlerle paylaşmak isteyebilirsiniz böylelikle diğerleri de yararlanabilir.

PERSONEL EĞİTİMİ:

\*Tüm personelin e güvenlik konularında düzenli eğitim alması öğrencilerinize gerçek bir fayda sağlamalıdır. Eğitimin orta ve uzun vadeli faydaları hakkında personelden geri bildirim almaya devam edin ve eğitim kursu önerisi için e güvenlik etiketi portalına danışın. (www.esafetylabel.eu/group/community/suggestions-for-online-training-courses)