



eSafety Label - Action Plan

Action plan submitted by Meryem Mehtap YILMAZ for DOĞANKÖY İLKOKULU - 18.11.2020 @ 11:10:57

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

Infrastructure

Technical security

An educational approach and building resilience in pupils of all ages is also key to safe and responsible online use so bring together all teachers to have a discussion on how they will talk to their pupils about being a good and safe digital citizen. See www.europa.eu/youth/EU_en for examples of discussions that can take place in the classroom on this topic, through role-play and group games.

Pupil and staff access to technology

All staff and pupils are allowed to use USB memory sticks in your school. This is good practice, and your Acceptable Use Policy should stipulate that all removable media is checked before use in the school systems. Check the fact sheet on Use of removable devices at www.esafetylabel.eu/group/community/use-of-removable-devices to make sure you cover all security aspects.

Since staff and pupils can use their own equipment on your school network, it is important to make sure that the Acceptable Use Policy is reviewed regularly by all members of the school and adapted as necessary. It must be discussed with pupils at the start of each academic year so that they understand what is in place to protect them and their privacy, and why. Base the policy around behaviour rather than technology. Visitors must also read and sign the Acceptable Use Policy before they use the school's network.

Data protection

It is good that your school provides materials on the importance of protecting devices, especially portable ones. Ensure that staff are aware of these and use them. This material should be pointed out to new staff as part of their induction. Please consider uploading those as evidence at [evidence](#) and sharing with others in the forum. Also ensure that your materials are regularly reviewed to ensure they are in line with the state of the latest technology.

You have a good policy of encrypting pupil data and storing it safely. Ensure all new staff made aware of the procedures for encryption and data handling and that there is a named point of contact acting as the data controller for

your school. Upload to your school profile some guidelines about protecting sensitive data through an encryption system so that other schools can benefit from your experience.

Okulumuzun e Güvenlik Eylem Planı

Doldurulmuş Değerlendirme Formunuzu e-Güvenlik Etiketini portalına göndererek, okulunuzdaki e-Güvenlik durumunu analiz etme yolunda önemli bir adım attınız. Tebrikler! Okulunuzda e-Güvenliği daha da geliştirmek için neler yapabileceğinizi görmek için lütfen Eylem Planınızı dikkatlice okuyun. Eylem Planı, 3 temel alana bölünmüş yararlı tavsiyeler ve yorumlar sunar: altyapı, politika ve uygulama.

Altyapı

Teknik güvenlik

Her yaşta öğrencide bir eğitim yaklaşımı ve dayanıklılık oluşturmak da güvenli ve sorumlu çevrimiçi kullanımın anahtarıdır, bu nedenle tüm öğretmenleri öğrencileriyle iyi ve güvenli bir dijital vatandaş olma konusunda nasıl konuşacakları konusunda bir tartışma yapmak için bir araya getirin. Rol yapma ve grup oyunları yoluyla bu konu hakkında sınıfta gerçekleştirilebilecek tartışma örnekleri için www.europa.eu/youth/EU_en adresini ziyaret edin.

Öğrenci ve personelin teknolojiye erişimi

Tüm personel ve öğrencilerin okulunuzdaki USB bellekleri kullanmasına izin verilir. Bu iyi bir uygulamadır ve Kabul Edilebilir Kullanım Politikanız, tüm çıkarılabilir ortamların okul sistemlerinde kullanılmadan önce kontrol edilmesini şart koşmalıdır. Tüm güvenlik hususlarını kapsadığınızdan emin olmak için www.esafetylevel.eu/group/community/use-of-removable-devices adresindeki çıkarılabilir cihazların kullanımı hakkındaki bilgi formunu kontrol edin.

Personel ve öğrenciler okul ağınızda kendi ekipmanlarını kullanabildikleri için, Kabul Edilebilir Kullanım Politikasının okulun tüm üyeleri tarafından düzenli olarak gözden geçirildiğinden ve gerektiği şekilde uyarıldığından emin olmak önemlidir. Her akademik yılın başında öğrencilerle tartışılmalıdır, böylece onları ve mahremiyetlerini korumak için neyin mevcut olduğunu ve nedenini anlasınlar. Politikayı teknolojiden çok davranışa dayandırın. Ziyaretçiler ayrıca okulun ağını kullanmadan önce Kabul Edilebilir Kullanım Politikasını okuyup imzalamalıdır.

Veri koruması

Okulunuzun, özellikle taşınabilir cihazlar olmak üzere cihazların korunmasının önemi hakkında materyaller sağlaması iyidir. Personelin bunlardan haberdar olmasını ve bunları kullanmasını sağlayın. Bu materyal, işe başlama sürecinin bir parçası olarak yeni personele belirtilmelidir. Lütfen bunları kanıt olarak yüklemeyi ve forumdaki diğer kişilerle paylaşmayı düşünün. Ayrıca, malzemelerinizin en son teknoloji ile uyumlu olduğundan emin olmak için düzenli olarak gözden geçirildiğinden emin olun.

Öğrenci verilerini şifreleme ve güvenli bir şekilde saklama konusunda iyi bir politikanız var. Tüm yeni personelin şifreleme ve veri işleme prosedürlerinden haberdar olduğundan ve okulunuz için veri denetleyicisi olarak görev yapan atlandırılmış bir iletişim noktası olduğundan emin olun. Diğer okulların deneyimlerinden yararlanabilmesi için, hassas verileri bir şifreleme sistemi aracılığıyla korumaya ilişkin bazı yönergeleri okul profilinize yükleyin.