YUNUS EMRE ANAOKULU
2022/2023 EĞİTİM ÖĞRETİM YILI
E-GÜVENLİK EYLEM PLANI

Altyapı

TEKNİK GÜVENLİK

- Bilişim hizmetlerinizin düzenli olarak gözden geçirilmesi ve artık kullanılmıyorsa kaldırılması iyi bir uygulamadır.
- Her yaştan öğrencide eğitimsel yaklaşım ve dayanıklılık oluşturmak güvenli ve sorumlu (bilinçli) çevrimiçi kullanımının olmazsa olmazıdır, bu nedenle iyi ve güvenli dijital vatandaş olma konusunda öğrencileriyle nasıl konuşacaklarını tartışmak için öğretmenleri bir araya gelir.

ÖĞRENCİ VE PERSONELİN TEKNOLOJİYE ERİŞİMİ

- Personel ve öğrenciler okul cihazları ile okul ağını kullanabildiği için, Kabul Edilebilir Kullanım Politikası'nın bütün okul üyeleri tarafından gözden geçirildiğinden ve gerekli durumlarda uyarlandığından emin olmak önemlidir. Politikayı teknolojiden ziyade davranışa dayandırmaktayız. Ağ kullanıcıları okul ağını kullanmadan önce 'Kabul Edilebilir Kullanım Politikası'nı okumalı ve okudum diye işaretlemeliler.

VERİ KORUMA

- Okulunuzun, özellikle taşınamaz cihazlar olmak üzere cihazların korunmasının önemi konusunda materyaller sağlaması iyidir. Personelin bunlardan haberdar olmasını ve bunları kullanmasını sağlayın. Bu materyal(akıllı tahtalar), işe başlamalarının bir parçası olarak yeni personele gösterilmelidir. Ayrıca materyallerimizin en son teknoloji ile uyumlu olduğundan emin olmak için düzenli olarak gözden geçirmekteyiz.
- Öğrenme ve yönetim ortamlarınızın bir arada olması bir güvenlik riski oluşturabilir. Personelin ve öğrencilerin özel verilerinin güvenliğini sağlamak okulun temel bir görevidir. Görevlendirdiğiniz e-Güvenlik müdürü/ BİT koordinatörünüzün, personel ve bir teknik uzmanla birlikte, öğrenme ve yönetim ortamlarını ayırmak veya aralarında eşdeğer en yüksek güvenlik düzeyini sağlamak için bir strateji tanımlamasını ve uygulamasını öneririz.

  E-posta sisteminizin korunması ve öğrenci verilerinin yerinde aktarımı için bir politikanızın olması iyidir.

Yazılım Lisansı

- Okulumuz, yazılım ihtiyaçları için gerçekçi bir bütçe belirler. Bu, iyidir. Bu şekilde kalmasını sağlayın. Bulut servisleri veya açık yazılımlar gibi alternatiflere de bakmak isteyebilirsiniz.
- Yeni yazılımın kurulumu için sahip olduğunuz etkili süreçler hakkında tüm yeni personele bilgi verilmesini sağlamak önemlidir. Bu sistemlerinizin güvenliğinin korunabileceği ve personelin öğretme ve öğrenmeye yardımcı olacak yeni yazılım uygulamalarını deneyebileceği anlamına gelir.

Bilgi Teknolojileri Yönetimi

- BİT ağında sorumlu kişinin, okulun sahip olduğu donanımda hangi yazılım bulunduğundan tam olarak haberdar olmasını sağlamak iyi bir uygulamadır ve bu,okul politikasında ve Kabul Edilebilir Kullanım Politikasında açıkça belirtilmelidir. Ağdan sorumlu kişinin, lisans gereksinimlerine uygunluğu garanti edebilmesi gerekir ve bu yeni yazılım ağın çalışmasını engellemeyecektir.
- Okul bilgisayarına yüklenen yeni yazılımın kullanımı ile ilgili eğitim almanız ve / veya rehberlik sağlamanız iyi bir uygulamadır. Bu, okul üyelerinin yeni özelliklerden yararlanmasını ve aynı zamanda ilgili yerlerde güvenlik ve veri koruma sorunlarının farkında olmalarını sağlar.

POLİTİKALAR

Kabul Edilebilir Kullanım Politikası (KKP)

- Okulunuzda, politika konuları düzenli olarak tartışılır. Bu, personelin ve öğrencilerin bunlardan haberdar olmalarını sağladığı için iyi bir uygulamadır. Öğrenciler ve personel de farkındalıklarını teyit etmek için ilgili belgeleri imzalamak zorunda mı?
- Okul topluluğunun tüm üyeleri için Kabul Edilebilir Kullanım Politikasına sahip olmanız iyi bir şey. Hala amaca uygun olduğundan emin olmak için KKP' yi düzenli olarak gözden geçirin; KKP' nizin yeterince kapsamlı olduğunda emin olmak için, bilgi formuna bakabilirsiniz.

Raporlama ve Olay Yönetimi Politikası

- Tüm personel, potansiyel olarak yasa dışı olabilecek materyallerle ilgilenme prosedürüne aşina mı? Bu tür bir vakada genel sorumluluk alan okul kıdemli liderlik ekibinden belirlenmiş bir kişi var mı? Prosedürün, Okul Politikasında tüm personele ve Kabul Edilebilir Kullanım Politikasında personel ve öğrencilere açıkça bildirilmesi gerekir.
- Yeni personel de dahil olmak üzere tüm personelin, bir okul makinesinde uygunsuz veya yasa dışı materyal bulunursa ne yapılacağına ilişkin yönergelerden haberdar olduğundan emin olun
- Lütfen E-güvenlik portalı içerisinde özellikle çocuk ve aile bağlamında ilişkili materyaller paylaşınız. Tüm Avrupa bünyesinde oluşturulan veri bankasına yaptığınız ve başarı sağlayan uygulamalarınızı paylaşmanız onların gelecekte kullanımını sağlayacaktır. Kabul Edilebilir Kullanım Politikası (AUP) konusunda çocukların giriş yaptığından emin olunuz. E-güvenlik olaylarını ele almada net bir okul Politikasına sahip olmanız iyi olacaktır. Toplum içerisinde farkındalığı arttıracak ve önleyici önlemler bağlamında tartışmak, ileri vadede sayıyı azaltmak için kullanılabilir.

Personel Politikası

Akıllı telefonlar ve diğer taşıyabilir cihazlar gibi yeni teknolojiler beraberinde bir dizi risk de getirirler. Temin ederiz ki öğretmenlerimizin bunun farkında. Bu sebeple bahsi geçen aletlerin tuzaklarından kaçabiliyor ve çocukların üzerinde bilgileri analiz edebiliyorlar.

Davranış Politikası

Çocuk davranışları ile ilgili düşüncelerimiz diğer okullar için de iyi bir örnek olabilir.

E-GÜVENLİK YÖNETİMİ

E-1güvenlik konuları için bağlantı sağlayan yönetici veya ana üyesi ile toplantılar düşünün ,olaylarla ilgili okul politikanız üzerinde gerçekleşen daha önceden derlediğiniz sayısal verileri paylaşın.

Müfredatta e-Güvenlik

Bu konunun e-güvenlik Müfredatı içerisinde incelenmesi iyidir.

Yeni olaylara karşı acil durum geliştirmek yerine E-güvenlik Eğitimi ile çevrelenmiş verilerin düzenli olarak incelenmesi daha iyidir

- E-Güvenlik'in okulunuzda müfredatın bir parçası olarak öğretilmesi faydalıdır. Tüm personelin sadece BİT veya Kişisel Sosyal ve Sağlık dersleri yoluyla değil, müfredat boyunca uygun olan yerlerde e-Güvenlik eğitimini sağladığından emin olun.
- Ulusal Güvenli İnternet'inizdeki çevrimiçi e-Güvenlik kaynaklarını sık sık kullandığınızı bilmekte fayda var.

Destek Kaynakları

- Ebeveynlerden kendileri için sağlanan e-Güvenlik desteği hakkında geri bildirim isteyin ve ondan yararlanan ve ona erişen ebeveynlerin sayısını en üst düzeye çıkarmanın yenilikçi yollarını düşünün. Ebeveyn akşamları için fikirler ve ebeveynlere iletilebilecek bilgi kaynakları için araştırmalar yapabilirsiniz.
- Tüm personelin e-Güvenlik konusunda bazı sorumlulukları olmalıdır. Okul danışmanları, vb. bu konularda tavsiye ve rehberlik etmeye, geliştirmeye ve okul politikanızı düzenli olarak gözden geçirmeye katkıda bulunmaya davet edilmelidir. Onların bilgi ve becerilerini maksimum düzeyde kullanın ve onlara eğitim vermenin uygun olup olmadığını düşünün.

Personel Eğitimi

- Okulunuzda personel arasında bilgi alışverişi teşvik edilmelidir. Bu bütün okul için faydalıdır. Kanıt aracı, okulum alanından da erişilebilen e-Safety konularında PowerPoint'leri, belgeleri veya bilgi alışverişlerinin benzerlerini yükleyin.

- Gönderdiğiniz Değerlendirme Formu geniş bir soru havuzundan oluşturulmuştur. Ayrıca ankette belirtilmeyen alanlarda e-Güvenliği iyileştirip iyileştirmediğinizi bilmekte faydalıdır. Bu tür değişikliklerin kanıtını, E-Güvenlik Portalı okul alanı bölümündeki Kanıtı yükle yoluyla yükleyebilirsiniz.