



DOĞANPINAR ŞEHİT COŞKUN TANRIÖVER İLKOKULU E-GÜVENLİK OKUL POLİTİKASI VE KURALLARI

Doğanpınar Şehit Coşkun Tanrıöver İlkokulu 07/2022 tarihine kadar bronz etikete sahiptir. Etiketimizi gümüş etiket seviyesine çıkarmak için **e-Safety** Label eylem planına uygun hareket edilecektir.

AMAÇ:

- Doğanpınar Şehit Coşkun Tanrıöver İlkokulu, e-güvenlik çalışmaları ile internet, bilgisayar, diz üstü bilgisayar ve cep telefonlarını kullanırken; öğrencilerin, velilerin ve öğretmenlerin korunmasını amaç edinmiştir.
- İnternetin ve teknolojinin yaşamın önemli bir parçası olması sebebiyle, herkes, riskleri yönetme ve strateji geliştirme yöntemlerinin öğrenilmesi konusunda bilinçlendirilmelidir.
- Politikamız, yöneticiler, öğretmenler, veliler, tüm personel ve öğrenciler için hazırlanmış olup, internet erişimi ve bilgi iletişim cihazlarının kullanımı için geçerlidir.

SORUMLULUKLAR:

- E-güvenlik politikalarının gelişmesine katkıda bulunmak.
- Olumlu öğrenme aşamasında mesleki gelişim için sorumluluk almak.
- Okulu ve içerisindekileri korumak için e-güvenlik konusunda sorumluluk almak.
- Teknolojiyi güvenli ve sorumlu kullanmak.
- Zarar görülmesi durumunda tehlikeyi gözlemleyip ilgili birimlere iletmek.

OKUL WEB SİTESİ:

- Doğanpınar Şehit Coşkun Tanrıöver İlkokulu olarak web sitemizde okulumuzun adres, telefon, fax ve e posta adres bilgileri bulunmaktadır.

- Sitemizde yayınlanan tüm içerikler okul müdürümüzün onayından geçtikten sonra bilgi işlem birimi tarafından siteye konulmaktadır.
- Okulumuzun web sitesi bilgi işlem birimimizin sorumluluğunda olup güçlü güvenlik önlemleri alınmış durumdadır.
- Öğrenci çalışmaları, velilerinin izinleriyle yayınlanmaktadır.

GÖRÜNTÜ VE VİDEOLARIN PAYLAŞIMI

- Paylaşılan tüm fotoğraf ve videolar okul politikasına uygun şekilde okul idaresinin izni ve onayı ile paylaşılmaktadır.
- Öğrenci içerikli tüm paylaşımlarda velilerin izinleri alınmaktadır.
- Veli izni yanında öğrencinin de izni olmadan fotoğrafı çekilip kullanılmamaktadır.

KULLANICILAR:

- Öğrenciler tarafından hazırlanacak olan bir video henüz hazırlanmadan önce, bununla ilgili görev alan öğrenciler, öğretmenlerinden izin almalıdır.
- Paylaşılan tüm öğrenci bazlı etkinliklerde, etkinlik öncesinde velilerin izinleri alınmalıdır.
- Video konferans, resmi ve onaylanmış siteler aracılığıyla yapılacaktır.
- Kullanıcılar, şahsi sosyal medya hesaplarında, okul öğrencileri ve çalışanlarının yer aldığı görselleri, okul yetkili mercileri tarafından onaylanmadan paylaşamazlar

İÇERİK:

- Video konferans yapılırken, tüm kullanıcıların katılabileceği siteler üzerinden yapılacaktır.
- Video konferans yapılmadan önce diğer okullarla iletişim kurulmuş olması gerekmektedir.
- Okul öğrenci ve çalışanlarını ilgilendiren/içinde bulunduran tüm içerik, ancak kontrol ve onay süreçlerinden geçtikten sonra, paylaşımına açık hale gelecektir.

İNTERNETİN VE BİLİŞİM CİHAZLARININ GÜVENLİ KULLANIMI:

- İnternet; bilgiye ulaşmakta en önemli araçlardan biri haline gelmişken, bunu okuldaki müfredat ile ilişkilendirerek doğru bilgiye en güvenli şekilde öğrencilerimizi ve öğretmenlerimizi ulaştırabiliyoruz.
- İnternet erişimlerimizi öğrencilerimizin yaş ve yeteneklerine göre entegre etmiş durumdayız.
- Tüm okulumuza ait bilişim cihazlarımızı kullanım politikamıza uygun şekilde, gerekli filtrelemeleri yaparak güvenli hale getirmiş durumdayız.
- Tüm çalışanlarımız, velilerimiz ve öğrencilerimiz etkili ve verimli çevrimiçi materyallerin kullanımı konusunda bilgilendirilmiştir.
- E-güvenlik ve siber zorbalık konuları belli derslerimizin yıllık planlarına dahil edilmiş olup, bu konularda yıl içinde öğrencilere bilgi aktarımı devam etmektedir.
- Çevirim içi materyaller öğretme ve öğrenmenin önemli bir parçası olup müfredat içinde aktif olarak kullanılmaktadır.
- 9 Şubat güvenli internet günü okulumuzda kutlanmaktadır.
- Okulumuz 5651 yasasına uygun güvenlik prosedürlerini tamamen uygulamaktadır, SOPHOS uygulamaları olan HARDWARE FIREWALL ve kurumsal bir yapıya sahip ANTIVIRUS uygulaması kullanılmaktadır. Ek olarak wi-fi için HOTSPOT güvenlik önlemi de sisteme dahil edilmiştir. Parola girişi sonrasında ek bir kullanıcı adı ve parola daha istemekle birlikte, kullanıcının mac adresinin sisteme kayıt edilmesini de gerektiren bir sistemdir.

CEP TELEFONLARI VE KİŞİSEL CİHAZLARIN KULLANIMI:

- Okul saatleri içinde öğrencilerimizin kişisel cep telefonu kullanımı yasaktır.
- Her türlü kişisel cihazların sorumluluğu kişinin kendisine aittir.
- Okulumuz bu tür cihazların kullanımından doğacak olumsuz sağlık ve yasal sorumlulukları kabul etmez.
- Okulumuz kişisel cep telefonlarının ve bilişim cihazlarının kayıp, çalınma ve hasardan korunması için gerekli tüm önlemleri alır fakat sorumluluk kişiye aittir.
- Okulumuz öğrencileri, velilerini aramaları gerektiği durumlarda okula ait olan telefonları bir okul idarecisi gözetiminde kullanabilirler.
- Öğrencilerimiz eğitim amaçlı (web 2.0 araçlarının kullanımı vb) kişisel cihazlarını kullanmak için okul yönetiminden izin almalıdır.
- Velilerimiz okul saatleri içerisinde öğrencileriyle görüşme yapmalarını gerektiği konusunda bilgilendirilirler. Eğer zorunlu haller var ise okul yönetiminden izin alarak görüşme yapmaları sağlanmalıdır.

- Öğrencilerimiz cep telefon numaralarını yalnızca güvenilir kişilerle paylaşmaları, tanımadıkları güvenilir bulmadıkları kişilerle cep telefonu gibi kişisel bilgilerini paylaşmamaları gerektiği konusunda bilinçlendirilmektedirler.
- Çalışanlar (öğretmen, idareci, personel vb) kişisel cep telefonlarını ders saatlerinde sessize alarak ya da kapatarak görevlerine devam etmelidir.
- Çalışanlar (öğretmen, idareci, personel vb) okul politikasına aykırı davranışlarda bulunursa disiplin işlemleri başlatılır.
- Kurum çalışanları (öğretmen, idareci, personel vb) ve öğrenciler sosyal medya ya da sohbet programları üzerinden öğrenci ya da kurum çalışanlarından gelecek olan ya da kendilerinin gönderecekleri her türlü içerik ve mesajlaşmanın hukuki sorumluluğunu taşımaktadır, uygunsuz olabilecek her türlü içerik ve mesajlaşma ivedilikle okul yönetimi ile paylaşılır. Böyle bir duruma mahal vermemek için gereken önlemler alınır.

E-GÜVENLİK EĞİTİMİ:

- Öğrenciler için e-güvenlik müfredatı ilgili derslerin yıllık planlarına eklenerek öğrenciler bu konularda bilgilendirilir.
- Tüm kullanıcıların internet kullanımları bilgi işlem birimi tarafından takip edilmektedir. Bu bilgi tüm kullanıcılara iletilmiştir.
- Öğrencilerimizin ihtiyaçları doğrultusunda çevirim içi güvenliği geliştirmek için rehberlik öğretmenleri ekran eğitimi uygulamaktadır.
- Teknolojiyi olumlu kullanan öğrenciler ödüllendirilecektir.
- Çevirim içi güvenlik politikası tüm çalışanlarımıza resmi olarak duyurulacaktır.
- 9 Şubat güvenli internet günü okulumuzda kutlanmaktadır. Bu güne yönelik okul koridorları ve sınıflarda pano çalışmalarımız ve sosyal medya paylaşımlarımız olur.

ÇEVİRİMİÇİ OLAYLAR VE KORUMA:

- Okulumuzun tüm üyeleri çevirim içi riskler konusunda bilgilendirilecektir. Eğitimler yapıp içerikler açıklanacaktır.
- Okulumuzda yasadışı içerik, güvenlik ihlali, siber zorbalık, cinsel içerikli mesajlaşma, çocuk istismarı, kişisel bilgi güvenliği gibi konularda bilgilendirme çalışmaları yapılmaktadır.
- 9 Şubat güvenli internet günü kutlanmaktadır.
- Okulumuzda internet, bilgi teknolojileri ve ekipmanlarının yanlış kullanımı ile ilgili tüm şikâyetler okul müdürüne bildirilecektir.
- Okulumuzun tüm üyeleri gizlilik ve güvenlik endişelerini ortadan kaldırmak için resmi okul kurallarına uygun şekilde davranmaları hususunda bilgilendirilir.

- Yaşanan olumsuzluklarda okul gerekli işlemleri yapmakla sorumludur.
- Sorunların çözümünde çalışanlar (öğretmen, idareci, personel vb), veliler ve öğrenciler okul ile birlikte hareket etmelidir.

İNTERNETTEKİ SOSYAL AĞLAR

İnternetin internetten ötesine taşınarak sosyal ağlar kullanılıyor. Sosyal ağlarda hangi kuralları kabul ettiğinizi gözden geçirin.

- Profilinizdeki görsel ve kullandığınız ayetlere dikkat edin.
- Sosyal medya arkadaşlarınızı dikkatle seçin.
- Sosyal ağ ortamında özel bilgilerinizi paylaşmayın.
- Paylaşacağınız yazı, resim, video vb. köşe yazıları paylaşmadan önce mutlaka kontrolünüzü yapın.
- Paylaşacağınız bilgiler için paylaşım ayarlarınızı kontrol edin.
- Sosyal medya sitesine katılmadan önce kuralları okuyun.
- Paylaşacağınız bilgileri yanlışlıkla paylaşmayın.

TANIMADIĞIN KİŞİLERLE ARKADAŞLIK KURMA !

İNTERNET KURALLARI VE SORUMLULUKLARINIZ

- İnternet ortamında gerçek ve hayalî kişilerle karşılaşabilirsiniz.
- Çeşitli amaçlarla kişilerin kimlik bilgilerini öğrenmek için kullanılmaktadır.
- İnternet ortamında her türlü bilgiyi paylaşmamaya dikkat etmelisiniz. Bu bilgilerinizi paylaşmadan önce mutlaka kontrolünüzü yapın.
- İnternet ortamında her türlü bilgiyi paylaşmamaya dikkat etmelisiniz. Bu bilgilerinizi paylaşmadan önce mutlaka kontrolünüzü yapın.
- İnternet ortamında her türlü bilgiyi paylaşmamaya dikkat etmelisiniz. Bu bilgilerinizi paylaşmadan önce mutlaka kontrolünüzü yapın.
- İnternet ortamında her türlü bilgiyi paylaşmamaya dikkat etmelisiniz. Bu bilgilerinizi paylaşmadan önce mutlaka kontrolünüzü yapın.

Bilgiyi Paylaşmadan Önce Düşün !

5 Şubat Güvenli İnternet Günü

Okullarımızda bu konuda birlikte çalışarak güvenli internet ortamını oluşturabiliriz. Bu konuda öğrencilerimizle birlikte çalışarak güvenli internet ortamını oluşturabiliriz.

5 Şubat Güvenli İnternet Günü

Okullarımızda bu konuda birlikte çalışarak güvenli internet ortamını oluşturabiliriz. Bu konuda öğrencilerimizle birlikte çalışarak güvenli internet ortamını oluşturabiliriz.



T.C Anayasasına,
Milli Eğitim Bakanlığımızın protokollerine,
Avrupa komisyonu eSafety hareket eylem planımıza,
Çocuk hakları beyannamesine,
Avrupa insan hakları beyannamesine göre

OKULUMUZDA İZİNSİZ FOTOĞRAF ÇEKEMEZSİNİZ



Bu, kiinin hak ve zgrlklerini ihlal eder

Milli Eğitim Bakanlığımızın protokollerine,
Avrupa komisyonu eSafety hareket eylem planımıza göre

OKULUMUZ ĐRENCİLERİ İZİNSİZ CEP TELEFONU ve TAŞINABİLİR AYGIT KULLANAMAZ



e SAFETY CHECK LIST

- CHECK YOUR FRIENDS LIST - DO YOU KNOW EVERYONE?
- DELETE ANY 'RANDOM' FRIEND REQUESTS THAT YOU MAY HAVE.
- BE CAREFUL WHAT YOU POST ONLINE! #CREATINGHATE
- MAKE SURE YOU SET YOUR PRIVACY SETTINGS TO FRIENDS ONLY.
- TELL SOMEONE, REPORT ABUSE, USE THE CEOP BUTTON, DON'T RESPOND, DON'T DELETE!





