eGüvenlik Politikamız

ŞEHİT YÜZBAŞI BEŞİR BAYRAKTAR İLKOKULU
E -GÜVENLİK OKUL POLİTİKASI ve KURALLARI

AMAÇ:

1. Şehit Yüzbaşı Beşir Bayraktar İlkokulu, e-Güvenlik çalışmaları ile İnternet, bilgisayar, dizüstü bilgisayar ve cep telefonlarını kullanırken; öğrencilerin, velilerin ve öğretmenlerin korunmasını amaç edinmiştir.
2. İnternetin ve teknolojinin yaşamın önemli bir parçası olması sebebiyle, herkes, riskleri yönetme ve strateji geliştirme yöntemlerinin öğrenilmesi konusunda bilinçlendirilmelidir.
3. Politikamız, yöneticiler, öğretmenler, veliler, tüm personel ve öğrenciler için hazırlanmış olup, internet erişimi ve bilgi İletişim cihazlarının kullanımı için geçerlidir.

SORUMLULUKLAR:

1. E-güvenlik politikalarının gelişmesine katkıda bulunmak.
2. Olumlu öğrenme aşamasında gelişim için sorumluluk almak.
3. Okulu ve içerisindekileri korumak için e-Güvenlik konusunda sorumluluk almak.
4. Teknolojiyi güvenli ve sorumlu bir şekilde kullanmak.
5. Zarar görülebilecek durumlarda tehlikeyi gözlemleyip ilgili birimlere iletmek.

OKUL WEB SİTESİ:

1. Şehit Yüzbaşı Beşir Bayraktar İlkokulu olarak web sitemizde okulumuzun adres, telefon, ve e-posta adres bilgileri bulunmaktadır.
2. Sitemizde yayınlanan tüm içerikler okul müdürümüzün onayından geçtikten sonra okulumuz web sitesi yayın ekibi tarafından siteye konulmaktadır.
3. Okulumuzun web sitesi okulumuz web yayın ekibinin sorumluluğunda olup güçlü güvenlik önlemleri alınmış durumdadır.
4. Öğrenci çalışmaları, velilerin izinleriyle yayınlanmaktadır.

GÖRÜNTÜ VE VİDEOLARIN PAYLAŞIMI:

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

KULLANICILAR:

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

İÇERİK:

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

İNTERNETİN VE BİLİŞİM CİHAZLARININ GÜVENLİ KULLANIMI:

1. İnternet; bilgiye ulaşmakta en önemli araçlardan biri haline gelmişken, bunu okuldaki müfredat ile ilişkilendirerek doğru bilgiye en güvenli şekilde öğrencilerimizi ve öğretmenlerimizi ulaştırabiliyoruz.
2. İnternet erişimlerimizi öğrencilerimizin yaş ve yeteneklerine göre uyarlamış durumdayız.
3. Tüm okulumuza ait bilişim cihazlarımızı kullanım politikamıza uygun şekilde, gerekli filtrelemeleri yaparak güvenli hale getirmiş durumdayız.
4. Tüm çalışanlarımız, velilerimiz ve öğrencilerimiz etkili ve verimli çevrimiçi materyallerin kullanımı konusunda bilgilendirilmiştir.

5. E-güvenlik ve siber zorbalık konuları belli derslerimizin yıllık planlarına dahil edilmiş olup, bu konularda yıl içinde öğrencilere bilgi aktarımı devam etmektedir.
6. Çevrimiçi materyaller öğretme ve öğrenmenin önemli bir parçası olup müfredat içinde aktif olarak kullanılmaktadır.
7. Güvenli internet günü okulumuzda kutlanmaktadır.
8. Okulumuz 5651yasasına uygun güvenlik prosedürlerini tamamen uygulamaktadır, tüm bilgisayarlarda ANTIVIRUS programları 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:

1. Okul saatleri içinde öğrencilerimizin kişisel cep telefonu kullanımı yasaktır. Gündüz cep telefonlarını müdür yardımcısına teslim eden öğrenciler akşam çıkış saatinde telefonlarını geri teslim alırlar.
2. Cep telefonunu yönetime teslim etmeyen ve cep telefonu ile okul içerisinde video ya da fotoğraf çeken öğrencilere yasaların ve Yönetmeliğin Ödül ve Disiplin maddeleri gereği işlem yapılmaktadır.
3. Her türlü kişisel cihazların sorumluluğu kişinin kendisine aittir.
4. Okulumuz bu tür cihazların kullanımından doğacak olumsuz sağlık ve yasal sorumlulukları kabul etmez.
5. Okulumuz kişisel cep telefonlarının ve bilişim cihazlarının kayıp, çalınma ve hasardan korunması için gerekli tüm önlemleri alır fakat sorumluluk kişiye aittir.
6. Okulumuz öğrencileri, velilerini aramaları gerektiği durumlarda okula ait olan telefonları bir okul idarecisi gözetiminde kullanabilirler.
7. Öğrencilerimiz eğitim amaçlı (web2 araçlarının kullanımı vb.) kişisel cihazlarını kullanmak için okul yönetiminden izin almalıdır.
8. Velilerimiz okul saatleri içerisinde öğrencileriyle görüşme yapmamaları gerektiği konusunda bilgilendirilirler. Eğer zorunlu haller var ise okul yönetiminden izin alarak görüşme yapmaları sağlanmalıdır.
9. Öğrencilerimiz cep telefon numaralarını yalnızca güvenilir kişilerle paylaşmaları, tanımadıkları ve güvenilir bulmadıkları kişilerle cep telefonu gibi kişisel bilgilerini paylaşmamaları gerektiği konusunda bilinçlendirilmektedirler.

10. Çalışanlar (öğretmen, idareci, personel vb.) kişisel cep telefonlarını ders saatlerinde sessize alarak ya da kapatarak görevlerine devam etmelidir.
11. Çalışanlar (öğretmen, idareci, personel vb) okul politikasına aykırı davranışlarda bulunursa disiplin işlemleri başlatılır.
12. Kurum çalışanları (öğretmen, idareci, personel vb.) ve öğrenciler sosyal medyada 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.

GÜVENLİK EĞİTİMİ:

1. Öğrenciler için e-Güvenlik müfredatı ilgili derslerin yıllık planlarına eklenerek öğrenciler bu konularda bilgilendirilir.
2. Çevrimiçi güvenlik politikası tüm çalışanlarımıza resmi olarak duyurulacaktır.
3. Güvenli internet günü okulumuzda kutlanmaktadır. Bugüne yönelik okul koridorları ve sınıflarda pano çalışmalarımız ve sosyal medya paylaşımlarımız olur.

ÇEVRİMİÇİ OLAYLAR VE KORUMA:

1. Okulumuzun tüm üyeleri çevirim içi riskler konusunda bilgilendirilecektir. Eğitimler yapılıp içerikler açıklanacaktır.
2. Okulumuzda yasa dışı içerik, güvenlik ihlali, siber zorbalık, cinsel içerikli mesajlaşma, çocuk istismarı, kişisel bilgi güvenliği gibi konularda bilgilendirme çalışmaları yapılmaktadır.
3. Okulumuzda internet, bilgi teknolojileri ve ekipmanlarının yanlış kullanımı iile lgili tüm şikayetler okul müdürüne bildirilecektir.
4. Okulumuzun tümü yeleri gizlilik ve güvenlik endişelerini ortadan kaldırmak için resmi okul kurallarına uygun şekilde davranmaları hususunda bilgilendirilir.
5. Yaşanan olumsuzluklarda okul gerekli işlemleri yapmakla sorumludur.
6. Sorunların çözümünde çalışanlar (öğretmen, idareci, personel vb.), veliler ve öğrenciler okul ile birlikte hareket etmelidir.

TÜM ÇALIŞANLARIN SORUMLULUKLARI ŞUNLARDIR:

1. Çevrimiçi güvenlik politikalarının geliştirilmesine katkıda bulunmak.
2. Okul sistemlerinin ve verilerin güvenliğinden sorumlu olmak.
3. Yeni ve gelişmekte olan teknolojiler kullanıldığında iyi uygulamaları modellemek.
4. Mümkün olduğunca müfredat ile çevrimiçi güvenlik eğitimini ilişkilendirmek.
5. Olumlu öğrenme fırsatlarına vurgu yapmak.
6. Bu alanda mesleki gelişim için kişisel sorumluluk almak.

ÇOCUKLARIN BAŞLICA SORUMLULUKLARI ŞUNLARDIR:

1. Çevrimiçi güvenlik politikalarının geliştirilmesine katkıda bulunmak.
2. Çevrimiçi ve çevrimdışı başkalarının hislerine ve haklarına saygı duymak.
3. İşler ters giderse, güvenilir bir yetişkinden yardım istemek ve çevrimiçi güvenlik sorunlarıyla karşılaşan diğer kişileri desteklemek.
4. Kendilerini ve başkalarını çevrimiçi olarak korumak için sorumluluk almak.
5. Belli bir teknolojiyi kullanmanın kişisel risklerini değerlendirmek ve bu riskleri sınırlamak için güvenli ve sorumluluk sahibi davranmak.

EBEVEYNLERİN BAŞLICA SORUMLULUKLARI ŞUNLARDIR:

1. Çocuklarıyla çevrimiçi güvenlik konularını tartışmak, okulun çevrimiçi güvenlik yaklaşımlarını desteklemek ve evde uygun güvenli çevrimiçi davranışları pekiştirmek.
2. Teknoloji ve sosyal medyanın güvenli ve uygun kullanımını modellemek.
3. Davranışlarında, çocuğun çevrimiçi olarak zarar görme tehlikesi altında olduğunu gösteren değişiklikleri belirlemek.
4. Okul veya diğer uygun kurumlardan, kendileri veya çocukları çevrimiçi problem veya sorunlarla karşılaşırsa yardım veya destek istemek.
5. Okulun çevrimiçi güvenlik politikalarının oluşturulmasına katkıda bulunmak.
6. Yeni ve gelişmekte olan teknolojilerin getirdiği fırsatlar ve risklerle ilgili olarak kendi bilinci ve öğrenimlerinden sorumlu olmak.

e-Güvenlik Bilgilendirme Çalışmaları

İnternet dijital dünyanın hızla gelişmesi ile birlikte insanoğlunun günlük yaşamının bir parçası haline gelmiştir. Ancak bir çok kolaylık sunmasının yanı sıra başta güvenlik ve gizlilik kaygıları olmak üzere çeşitli riskleri de beraberinde getirmektedir. Çocuklarımızın teknolojiden olumsuz olarak etkilenmesini önlemeyi hedef alarak dijital alanları ihtiyaçları doğrultusunda kullanmalarını destekliyoruz. Bu doğrultuda tüm öğrencilerimizin e-Güvenlik hakkında bilgi sahibi olmalarını önemsiyoruz.

6 adımda güvenli internet kullanımı hakkında bilgi almak için Tıklayınız.

EBA,Canlı Ders,EBATV,Akademik Destek,Mesleki Gelişim,Eğitim Bilişim Ağı

Çevrimiçi güvenlik ipuçları için Tıklayınız.

ÇEVRİMİÇİ GÜVENLİK İPUÇLARI

Tek başına veya başkalarına karşı çevrimiçi oyun oynamak, basit arcade oyunlarından, aynı anda tek bir çevrimiçi oyuna katılan çok sayıda oyuncunun yer alabileceği çok oyunculu çevrimiçi oyunlara (MMO) kadar standart mod olmuştur. Bu MMO'ların çoğu sanal toplulukları desteklemektedir ve bu, oyuncuları bilinmeyen diğer oyuncularla gerçek zamanlı etkileşim ile ilgili risklere maruz bırakabilir.

Bu riskler şunları içerir:

- Oyunda yaratılan ve gençler için uygun olmayan kullanıcı tarafından oluşturulan içerik ve oyuna verilen yaş sınırı ile uyuşmazlık.
- Bazı oyuncular gençler için uygun olmayan davranışlarda bulunurlar. Örneğin, uygunsuz veya saldırgan bir dil; metin, ses veya video iletişimine izin veren oyunlarda zorbalık; hile ve kurcalama gibi sportmenlik dışı davranış; veya başkalarına karşı saldırganlık.
- Mahremiyetin ihlali. Çevrimiçi oyun, çocuklar da dahil olmak üzere, insanları anlamlı ilişkiler kurmaya teşvik edebilir; ancak bu, kişisel ayrıntıları paylaşma veya oyun dışında bilinmeyen diğer oyuncularla tanışma riskini beraberinde getirir.
- İçeriğin gençler için uygun olmadığı web sitelerine bağlantılar.

AİLE İÇİN GÜVENLİK İPUÇLARI

- Çocuğunuza diğer oyunculara kişisel detayları vermemeleri gerektiğini açıklayın.
- Çocuğunuza, eşlik etmediğiniz sürece diğer oyuncularla tanışmaması gerektiğini söyleyin.
- Çocuklarınızın etkinliklerini oyun web sitelerinde izleyin. Daha da iyisi onlarla oyna birlikte oynayın.
- Çocuğunuza zorbalık, tehdit edici veya kötü dil, istenmeyen içeriğin gösterilmesi veya oyun dışında buluşma davetleri gibi sorunları bildirmeleri için teşvik edin ve hatırlatın.
- Bu sitedeki geribildirim sayfasını veya konsollardaki veya oyunların web sitelerindeki belirli şikayet mekanizmalarını kullanarak uygunsuz davranışı bildirin.
- Oyundaki herhangi bir şey geliştiği şekilde takdirde iletişimi bırakın ya da çocuğunuzun çevrimiçi kimliğini değiştirin.

ÇOCUKLAR İÇİN GÜVENLİK İPUÇLARI

- Kötü davranış, kötü dil veya hile doğru değildir! Sizi rahatsız eden oyuncuların sizinle iletişim kurmasını engelleyebilir, onları oyun sağlayıcıya veya platforma bildirebilir veya ailenize söyleyebilirsiniz.
- Sizi rahatsız eden herhangi bir bilgiye rastlarsanız, ailenize derhal söyleyin.

- Ev adresiniz, e-posta adresiniz, telefon numaranız, şifreleriniz veya resimleriniz gibi kişisel bilgileri vermeyin.
- İlk önce ailenizle görüşmeden çevrimiçi tanıştığınız birisiyle bir araya gelmeyi asla kabul etmeyin.

Resmi Yazılar ve Dökümanlar

eTwinning ve e-Güvenlik ile ilgili yayınlanan resmi yazılara aşağıdaki bağlantılardan ulaşabilirsiniz.

Milli Eğitim Bakanlığı Bilgi ve Sistem Güvenliği Yönergesi için Tıklayınız.

1955.pdf (meb.gov.tr)

Okullarda Sosyal Medyanın Kullanılması ile ilgili genelge için Tıklayınız.

1833.pdf (meb.gov.tr)

eTwinning Faaliyetlerinin Yaygınlaştırılması konulu resmi yazı için Tıklayınız.

eTwinning-Faaliyetinin-Yayginlastirilmasi.pdf (eba.gov.tr)

Aile Çocuk İnternet Kullanım Sözleşmesi için Tıklayınız.

10125751_anne_baba_cocuk_sozleYmesi.pdf (meb.k12.tr)

Güvenli internet Günü Nedir?

Avrupa Komisyonu'nun Güvenli İnternet Programı çerçevesinde, Güvenli internet ağı, 2004 yılından bu yana her Şubat ayında ve eş zamanlı olarak, Avrupa ve dışındaki ülkeleri kapsayarak, Güvenli İnternet Günü, düzenlemektedir.

Güvenli İnternet Günü (SID) özellikle dünya çapında çocuk ve gençler arasında online teknoloji ve cep telefonları ile daha güvenli ve sorumlu bir şekilde kullanımını teşvik etmek için her yıl Şubat ayında insafe tarafından organize edilmektedir.

e-Güvenlik Etiketi; okullara, eğitim ve öğretim deneyiminin parçası olarak çevrimiçi teknolojilere güvenli bir şekilde erişim sağlayarak güvenli ve zenginleştirici bir ortam sağlama görevlerinde yardımcı olmayı amaçlamaktadır. Ayrıca, politikacıların okullarda karşılaşılan e-Güvenlik sorunlarını daha iyi bir şekilde anlamalarını sağlamaktadır. İnternet sitesi: www.esafetylabel.eu

eTwinning ve e-Güvenlik Arasındaki İlişki Nedir?

e-Güvenlik; eTwinning yolculuğu sırasında internetin olumlu, güvenli ve etkin kullanımıyla ilgili konular ve fırsatlar hakkında bilgiler, iyi uygulamalar ve kılavuzlar sunar.

eTwinning 2005 yılında başladığından beri; internetin sorumlu bir şekilde kullanımını teşvik etmiş, öğretmenlerin ve öğrencilerin çevrimiçi olarak işbirliği yapmaları için güvenli bir ortam geliştirmiştir.

Avrupa'daki okullara ağ ve işbirliği için güvenli bir çevre sağlamak eTwinning' in en önemli önceliğidir.Çalışmanın büyük çoğunluğu çevrimiçi olarak yapıldığından, öğretmenler ve öğrenciler çalışmalarının özel olarak kalabileceği ve dış kullanıcıların erişemeyeceği korunmuş bir alanda güvence altındadır.

eTwinning platformu, Internet güvenliğinin çok büyük bir rol oynadığı alanlara sahiptir:

– eTwinning Masaüstü: Öğretmenler bağlantı sağlayabilir, ağa bağlanabilir, kaynakları paylaşabilir ve gelecekteki proje çalışmaları için plan yapabilirler.

– eTwinning TwinSpace: Öğretmenler ve öğrenciler işbirlikçi bir projede birlikte çalışırlar.

Bu kısıtlı alanların her ikisi de ve bunlara ilişkin araçlar kullanıcı adı ve şifre ile koruma altındadır. eTwinning ekibi bu güvenlik düzeyinin en üst seviyede olduğunu garantiler ve hatta okul saatleri dışında evden çalışan öğretmen ve öğrenciler de güvence altındadır.

eTwinning ekibi, INSAFE (www.saferinternet.org), ile yakın temas halinde çalışmıstır, bu Internet ve mobil araçların genç insanlar tarafından güvenli bir şekilde kullanımını teşvik eden, Avrupa Bilinçlenme Merkezleri Ağı'dır.

Öğretmen olmayan kullanıcılar ya da sahte isimlerle kullanıcı hesabı oluşturanlar, portaldan silinmektedir. Portalda bu tür davranışların bilgi güvenliği ve internet etiği açısından suç teşkil ettiğini hatırlatmak isteriz.

İnterneti Güvenli Kullanmak için 5 önemli ipucu:

1- Bilgi güvenliğiniz için güçlü bir parola oluşturduğunuzdan emin olun.

2- Güvenliğinizi sağlamak için gizlilik ayarlarınızı en üst seviyede tutun.

3- En son güvenlik yazılımlarınızın güncel olduğundan emin olun.

4- Masaüstü veya dizüstü bilgisayarlarımızda gösterdiğimiz güvenlik hassasiyetimizi cep telefonlarınız için de göstermeyi unutmayın.

5- Güvenmediğiniz bağlantılara tıklamayınız.


T.C. Anayasasına,
Milli Eğitim Bakanlığımızın protokollerine,
Avrupa Komisyonu eSafety hareket eylem planımıza,
Çocuk Hakları Beyannamesine,
Avrupa İnsan Hakları Beyannamesine göre,
eTwinning
OKULUMUZDA İZİNSİZ FOTOĞRAF ÇEKEMEZSİNİZ
Bu, kişinin hak ve özgürlüklerini ihlal eder.
ÇÖZÜM
LGS'ye
Başarıya Giden Yol
ÇÖZÜM'le Başlar
15
MART pazar
ÜCRETSİZ BURSLULUK SINAVI