

T.C.

Osmangazi Kaymakamlığı

Osmangazi Milli Eğitim Müdürlüğü

Necatibey Mesleki ve Teknik Anadolu Lisesi

e-Güvenlik Okul Eylem Planı

Tarih 22.12.2022-Saat: 15.00

1. Altyapı

Teknik Güvenlik

Okul internet ağıımız güvenlidir. Okulumuz, MEB Fatih Projesi kapsamındadır. Fatih Projesinin beş bileşeni bulunmaktadır. Bilinçli, güvenli, yönetilebilir ve ölçülebilir bilişim teknolojileri kullanımı beşinci bileşen olarak projede yer almaktadır. Bu bileşen hem fiziksel güvenliği hem de güvenli bilinçli internet kullanımını kapsamaktadır.

Milli Eğitim Bakanlığı, okullara Bilişim Teknolojileri sınıfı ve Türk Telekom A.Ş. ile yaptığı işbirliği protokolü ile akredite bir internet servis sağlıyor. Okulumuzda sunulan internet erişiminde filtreler kullanarak uygunsuz sitelere erişim engellemektedir. Bu şekilde çocukların interneti hem güvenli kullanması hem de eğitsel kullanımının dışına çıkmaması hedeflenmektedir.

Okulumuzda, Fatih Projesi kapsamında, İnternet erişimi izlemesi yapılmaktadır.

Okulumuzdaki bilgisayarların virüs koruma ve bakımları haftalık ve aylık olarak, okulumuzun anlaşmalı olduğu firma ile düzenli olarak yapılmakta. Anlaşma gereği Okulumuz Teknik Müdür Yardımcısı ile sürekli iletişim halindedir. Bilişim Atölyeleri ve Bilgisayarların bakımı ile Teknik Müdür Yardımcımız ilgilenmektedir.

Okulumuz Mesleki ve Teknik Anadolu Lisesi olduğu için beş farklı alan mevcuttur. Her alanın Alan Şefi ve Atölye Şefleri vardır. Şefler, Bilgisayar Laboratuvarı ve bilgisayarların ISG kapsamında yapılması gereken işleri, virüs koruması, bakımı ve onarımları konusunda Teknik Müdür Yardımcımıza destek olmaktadır. Ayrıca Bursa İl Milli Eğitimden Fatih Projesi danışmanımız mevcuttur.

Öğrencilerin ve Personelin Teknolojiye Erişimleri

Okulumuz e-Güvenlik Politikası kapsamında öğretmenleri, iyi ve güvenli bir dijital vatandaş olma konusunda öğrencilerimizle nasıl konuşacakları konusunda bir beyin fırtınası yapmak için bir araya getirir. Amacımız, öğrencilerimize sorumlu çevrimiçi kullanım bilincini geliştirmektir. Öğrenciler, zararlı sitelere giriş yapmak istediklerinde, Milli Eğitim Bakanlığının Protokolü kapsamında (Covid 19 süreci ile birlikte) YouTube dışında hiçbir sosyal medya hesabı açılmayacağı mesajını alacakları konusunda öğretmenler tarafından bilgilendirilmektedir. İnternet kullanımımız Milli Eğitim Bakanlığının 2017-12 Sayılı Okullarda Sosyal Medyanın Kullanılması Genelgesine uygundur.

Fatih Projesi kapsamında personele dağıtılan tabletler sadece EBA ve eklentilerini açmaktadır. Farklı bir içerik ya da mobil uygulama yüklenmemektedir. Personelimiz, Akıllı Tahtayı Anahtar USB ile açabilmektedir. Ders içerikleri için ayrıca bir USB kullanılmaktadır. Öğrencilerin, sadece öğretmen denetiminde akıllı tahtaya USB takmasına izin verilir. USB takıldığında virüs koruma programı uyarı vermektedir. Uygunsuz içerik ya da virüs varsa, filtreleme olduğu için içerik açılmamaktadır. Virüs programları düzenli olarak güncellenir. Okulumuz Akıllı Tahtalarında EBA-ÖBA ve e-okul içerikleri kullanılmaktadır. Öğrencilerimizin, Akıllı Tahtaya MP3 takmalarına okul idaresi ve personelimiz izin

vermez. Akıllı Tahtalarımızda, bilgisayarlarımızda CD ve DVD girişi yoktur.

Okul içerisinde video ya da fotoğraf çekmek yasaktır. Fotoğraf çeken öğrencilere yasalar ve Ödül ve Disiplin Yönetmeliği maddeleri gereği işlem yapılmaktadır. Öğrencilerimiz eğitim amaçlı (web 2 araçlarının kullanımı vb) kişisel cihazlarını kullanmak için okul yönetiminden izin alırlar. Okulumuz öğrencileri, velilerini aramaları gerektiği durumlarda okula ait olan telefonu bir okul idarecisi gözetiminde kullanabilirler.

Okulumuz kişisel cep telefonlarının ve bilişim cihazlarının kayıp, çalınma ve hasardan korunması için gerekli tüm önlemleri alır fakat sorumluluk kişiye aittir. Her türlü kişisel cihazların sorumluluğu kişinin kendisine aittir. Okulumuz bu tür cihazların kullanımından doğacak olumsuz sağlık ve yasal sorumlulukları kabul etmez.

Çalışanlar (öğretmen, idareci, personel vb) kişisel cep telefonlarını ders saatlerinde sessize alarak ya da kapatarak görevlerine devam eder. 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.

Veri koruması

Okul yönetimi ve personelimiz tarafından öğrenci verileri e-Okul Yönetimi Bilgi Sistemine yüklenir. e-okul Veli Bilgilendirme Sistemi ile de veliye bilgi verilir. e-okul portalına okul yönetimi-personel - öğrenci ve veli şifre ile giriş yapabilir. Şifreler belirli aralıklarla düzenli olarak değiştirilir. Öğrenci verileri üçüncü kişilerle paylaşamaz. Paylaşıldığı takdirde Disiplin ve Ceza Yönetmeliğine uygun olarak cezalandırılır.

EBA Platformunda da öğrenci verileri sınırlı bir şekilde kullanılır. EBA'da amaç öğrencinin akademik olarak gelişimini sağlamaktır. Ders öğretmenleri görür ve uygun bir şekilde öğrenciye Geri Bildirim verir.

Okulumuzun e-posta adresi iki tanedir. Kamu yazışmaları için kullanılan adres ve personel-öğrenci ve veli için kullanılan mail adresi. Okulumuz e-posta adresinin şifresi düzenli aralıklarla güncellenir. Okulumuz e-posta adresi şifresi sadece okul yönetimince kullanılır. 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 kullanımını konusunda bilgilendirilmiştir.

Yazılım Lisansı

Okulumuz bilgisayarlarında, anti-virüs koruması ve güvenlik duvarları tüm okul cihazlarında kuruludur ve düzenli olarak güncellenir.

Okul makinelerinde kullanılan web tarayıcılarının güvenlik ayarlarını kişiselleştirerek istenmeyen web sitelerini ve açılır pencereleri engellenmiştir. Öğrencilere bunun neden yapıldığını açıklanmıştır ve bunun onların korunması için olduğunu açıkça belirtilmiştir.

Bilişim Teknolojileri (BT) Yönetimi

Okul bilgisayarlarımıza, Fatih Projesi kapsamında olduğundan dolayı; proje protokolleri doğrultusunda hareket edilir.

Yeni donanım konusunda, Okul Müdürümüz, Teknik Müdür Yardımcımız, Alanlarımızın; Alan ve Atölye Şefleri sorumludur. Grafik ve Fotoğraf Alanımız, Tekstil Teknolojisi Alanımız, Moda Tasarımı Alanımız farklı programlar kullanmaktadırlar. Bu yeni yazılımlar, öğretmenlere derslerde daha ilgi çekici ders oluşturmalarına imkânı sağlıyor. İşletmelerde Mesleki Eğitim dersi kapsamında İşletmelerin ihtiyaçları için de öğrencilerimiz hazır durumda oluyor.

2. Politika

Kabul Edilebilir Kullanım Politikası (AUP)

Okulumuzun bilgisayar sistemlerini yüzlerce kullanıcı paylaşmaktadır. Bu sistemler dikkatli bir şekilde kullanılmalıdır; birkaç kişinin hatalı kullanımı bile okulun ve diğer kişilerin çalışmalarını sekteye uğratma potansiyeline sahiptir. Bu sebeple kullanıcılar okulun bilgisayar sistemlerini kullanırken dikkatli olmalı ve etik davranış sergilemelidir. Bu yükümlülük, aşağıdakilerle sınırlı olmamakla birlikte şunları kapsamaktadır:

Necatibey Mesleki ve Teknik Anadolu Lisesi Kabul Edilebilir Kullanım Politikası veya bilgisayar sistemlerin kullanımına ilişkin olarak kullanıcılara sadece bilgisayar sistemlerinin kullanımına ilişkin sınırlı bir lisans tanımaktadır. Kullanıcılar bilgisayar sistemlerinin hiçbir yazılım veya diğer bir parçasını kopyalayamaz, değiştiremez, yeniden üretmez. Bunlardan yeni bir çalışma yaratamaz, tersine mühendislik yapamaz, parçalara ayıramaz veya diğer bir şekilde kaynak koduna dönüştüremezler.

Kullanıcılar, okulumuzun izin vermediği bilgisayar sistemlerini kullanamazlar. Bilgisayar sistemlerine erişebilmek için hatalı veya aldatıcı bilgilerin temin edilmesi suretiyle veya benzer şekillerde bilgisayar sistemlerinin yetkisiz kullanımı yasaktır. Kullanıcılar diğer kurum, kuruluş veya kişilerin bilgisayar sistemlerine yetkisiz erişim sağlamak için okulumuzun bilgisayar sistemlerini kullanamazlar.

Kullanıcılar, okul hesaplarını kullanması için hiç kimseyi hiçbir sebeple yetkilendiremez. Okul hesabının her türlü kullanımından hesap sahibi sorumludur. Kullanıcılar hesaplarının yetkisiz kişilerce kullanılmasının önüne geçilmesi için şifre koruma ve belge koruma dâhil tüm önlemleri almalıdır. Şifrelerini başka bir kişiyle paylaşmamalı ve şifrelerini düzenli olarak değiştirmelidir. Bir kullanıcı hesabına ait şifre kullanılarak gerçekleştirilen her türlü işlem, söz konusu işlemi gerçekleştiren taraf hesap sahibinin kendisi olmasa dahi sorumlu hesap sahibidir.

Okulun bilgisayar sistemleri yalnızca izin verildiği şekilde okul ile ilgili konularda kullanılmalıdır. Tüm okul donanımı için söz konusu olduğu üzere, okul ağı dâhil bilgisayar sistemlerinin şahsi veya ticari amaçlar doğrultusunda kullanılması, açıkça izin verilmeyen haller dışında yasaktır. Okulun bilgisayar sistemleri, hileli ya da hukuka aykırı bir şekilde elde edilmiş medya belgeleri ile yazılımların toplanması, yüklenmesi, dağıtılması dâhil ve bunlarla sınırlı olmamak üzere hiçbir hukuka aykırı amaç için kullanılamaz. Dış ağ veya hizmetlerin – bulut hizmetleri dâhil – kullanımı hem okul hem de söz konusu ağ ve hizmetleri sunan kuruluşlar tarafından yayınlanan kabul edilebilir kullanım politikalarına uygun olmalıdır.

Kullanıcılar okulun ilgili personeli, bilgi güvenliği sorumlusu veya ilgili taraftan önceden izin almadıkça, herhangi bir bilgiye, okula ait yazılıma veya diğer belgelere (programlar, altyordam kitaplığı üyeleri, veri ve elektronik posta dâhil) erişemez; söz konusu bilgi, yazılım ve belgeleri değiştiremez, kopyalayamaz, taşıyamaz veya kaldıramaz. Kullanıcılar lisans verenden önceden izin almadıkça, üçüncü kişilere ait yazılımları kopyalayamaz, dağıtamaz, görüntüleyemez veya açıklayamaz. Kullanıcılar kullanımı için uygun bir şekilde lisanslanmamış olan yazılımları sistemlere yükleyemez.

Okul Personeli, parolada asla kişisel tanımlayıcı bilgiler kullanılamazlar. Buna isimler, doğum tarihleri, evcil hayvanlar, sokak adresleri, okullar, telefon numaraları, plaka numaraları vb. dâhildir.

Bunlar, hesaplarına erişmeye çalışan herkes için ilk tahminler olacaktır. Kullanıcılar gerçekten şifrelerini yazmaları gerektiğini düşünüyorsa, bu, erişim sağladığı cihazdan çok uzak tutulmalıdır.

Okula ait hiçbir bilgisayar sistemi sorumsuz bir şekilde veya başkalarının işlerine engel olacak şekilde kullanılamaz. Hakaret içerikli, rahatsız edici veya taciz edici içerikler ile zincirleme mektup, yetkisiz toplu mail veya istenmeyen reklamların iletilmesi veya ulaşılabilir kılınması. Sistem kaynaklarının kasıtlı olarak hatalı kullanılması veya başkalarının hatalı kullanmasının sağlanması veya ücretsiz yazılım gibi güvenilir olmayan kaynaklardan idari sistemlere yazılım veya veri indirilmesi.

Okul, bilgisayar sistemlerine bizzat sağlamadığı içeriklerden hiçbir şekilde sorumlu değildir. Kullanıcılar başkaları tarafından verilen içeriklere, bunların hakaret içerici, uygunsuz veya sakıncalı olduğunu düşünebileceğini kabul ederek ve risk kullanıcının kendisine ait olmak üzere erişir. Bilgisayar sistemleri "Olduğu Gibi" ve "Mevcut Haliyle" sunulmaktadır. Okul, üçüncü taraf içeriklerinin doğru, tam ve güvenilir olduğuna ilişkin her türlü yükümlülükten kendini muaf tutmaktadır. Kullanıcı bilgisayar sistemlerinde bulundurduğu veya sakladığı bilgilerden kendisi sorumludur.

Kullanıcı (I) bilgisayar sistemlerinin işleyişini veya söz konusu bilgisayar sistemlerinin başkaları tarafından kullanımını engelleyici her türlü harekete teşebbüsün; (II) bilgisayar sistemlerine fazla yüklemeye yapacak içeriklerin yüklenmesinin; (III) bilgisayar sistemlerinin genel güvenliğine tehlike arz edecek ve/veya diğer kullanıcıları zarara uğratabilecek hareketlerin; (IV) bilgisayar sistemlerinin işleyişini engelleyici veya müdahale edici yazılımların kullanılmasının veya kullanılmaya çalışılmasının mutlak bir biçimde yasak olduğunu kabul eder.

İşbu politikanın başka bir kişi tarafından ihlaline veya bilgisayar sistemlerinin güvenliği ile ilgili bir hata ya da güvenliğin ihlal edilmesine ilişkin her türlü bilginin tespiti durumunda, vakanın Bursa Necatibey Mesleki ve Teknik Anadolu Lisesi e-Güvenlik Koordinatörüne bildirilmesi zorunludur.

Okul bilgisayar sistemlerinin yetkisiz veya uygunsuz bir şekilde kullanımı, işbu politikaya uyulmaması dâhil, okul politikasının ihlalini teşkil etmektedir. İşbu politikaya veya politikanın belli bir duruma uygulanmasına ilişkin her türlü bilginin tespiti durumunda vakanın, Bursa Necatibey Mesleki ve Teknik Anadolu Lisesi e-Güvenlik Koordinatörlüğüne iletilir.

Yasadışı içerikler, şüphelendiğimiz durumları ihbarweb.org.tr sayfasından raporlama yapılır.

Raporlama ve Olay İşleme

Okulumuz tüm personeline, potansiyel olarak yasa dışı olabilecek materyallerle başa çıkma prosedürü hakkında bilgi verilir. Bu tür bir durumda genel sorumluluk alabilecek okul üst düzey lideri Okul Müdürüdür. Prosedür, okul politikasındaki tüm personele ve Kabul Edilebilir Kullanım Politikasındaki personel ve öğrencilere açıkça iletilmiştir.) Yasadışı içerikler, şüphelendiğimiz durumları ihbarweb.org.tr sayfasından raporlama yapılır.

Zorbalık olaylarına uygulanan detayları ve çözümleri hem çalışanlar hem de eSafety Label olay işleme formu aracılığıyla paylaşılır. Bu şekilde deneyim kazanılır ve başkalarının benzer olayları ele alma uygulamaları öğrenilir. Ayrıca, Kabul Edilebilir Kullanım Politikamızdaki zorbalıkla mücadele kuralları öğrencilere ve personele iletilir.

Personel Politikası

Personeler parolalar okul bilgi işlem sistemine veya bireysel cihazlara benzersiz giriş noktaları sunar ve bazı temel parola güvenliği kuralları titizlikle hatırlatılır.

Personeler güvenli bir şifre oluşturmanın 4 altın kuralını hatırlatılır: Şifre ideal olarak 10 ila 14 karakter arasında uzun ve karmaşık hale getirilir. Rakamlar, semboller, büyük ve küçük harflerin ve noktalama işaretlerinin bir karışımını kullanılır. Hatırlamaya yardımcı olması için anımsatıcı cihazlar kullanılır. Örnek olarak "Kızım Harriet harika bir tenisçidir" gibi bir cümlenin kısaltması "Md,h,=gr8tP" veya "Her gün yağmurda şarkı söylemeyi seviyorum!" olur "I<3SitR364!"

Personeler, parola asla kişisel tanımlayıcı bilgiler kullanılmayacakları belirtilir. Buna isimler, doğum tarihleri, evcil hayvanlar, sokak adresleri, okullar, telefon numaraları, plaka numaraları vb. dâhildir. Bunlar, hesaplarına erişmeye çalışan herkes için ilk tahminler olacaktır. Bir şifre diş fırçası gibidir, asla paylaşılmamalı ve sık sık değiştirilmelidir! Kullanıcılar gerçekten şifrelerini yazmaları gerektiğini düşünüyorlarsa, bu, erişim sağladığı cihazdan çok uzak tutulmalıdır.

Parola yönetimiyle ilgili temel kuralları Kabul Edilebilir Kullanım Politikamıza dâhil ettik. Öğretmenler, kaydoldukları hesabın bir hatırlatıcısı olarak sık sık sınıflarıyla AUP'ye bakmaya davet edilir.

Öğrenci Uygulaması / Davranışları

Öğrenciler zorbalık ve gizlilik ihlali gibi çevrimiçi sorunların olası sonuçları hakkında bilgilendirmek için okulda farkındalık yaratma etkinlikleri düzenlenir. Öğrenciler için sorumluluklar belirlenir. Çevrimiçi güvenlik politikalarının geliştirilmesine katkıda bulunur. Çevrim içi ve çevrim dışı başkalarının hislerine ve haklarına saygı gösterir. İşler ters giderse, ailesi öncelikli olmak üzere güvenilir bir yetişkinden yardım ister ve çevrimiçi güvenlik sorunlarıyla karşılaşan diğer kişileri destekler. Bireysel olarak, yaşlarına, yeteneklerine ve zayıf yönlerine uygun bir seviyede; kendilerini ve başkalarını çevrimiçi olarak korumak için sorumluluk almak. Yeni ve gelişmekte olan teknolojilerin getirdiği fırsatlar ve risklerle ilgili olarak kendi bilinci ve öğrenimlerinden sorumlu olmak. Belli bir teknolojiyi kullanmanın kişisel risklerini değerlendirmek ve bu riskleri sınırlamak için güvenli ve sorumluluk sahibi davranmak.

Personeler çevrimiçi sorunlarla nasıl daha iyi başa çıkılabileceği konusunda yıllık eğitim düzenlenir. Raporların sayısı ve niteliği takip edilir ve okulumuzdaki özel ihtiyaçları belirlenir. Okulumuzdaki eSafety uygulamaları tartışılırken, öğrencilerden geri bildirimler gelebilir. Öğrenciler mümkün olduğu kadar işleyişe dâhil edilir. Böylece öğrenciler gerçek hayattaki sorunları daha yakından tanırlar.

Online Okul Varlığı

Okul Müdürü sorumluluğunda, Baş Müdür Yardımcısı, Türk Dili ve Edebiyatı Öğretmeni, Grafik ve Tasarım alanı öğretmeninden oluşan Okul İnternet Sitesi Yayın Ekibimiz bulunmaktadır.

İnternet (Web) sitesinde iletişim bilgileri okul adresi, e-posta ve telefon numarası olacaktır. Personel veya öğrencilerin kişisel bilgileri yayınlanmayacaktır. Kullanımın gerekli olduğu durumlarda ise açık liste kullanılacaktır.

Okul Müdürü yayınlanan çevrimiçi içerik için genel yayın sorumluluğunu alacak ve bilgilerin doğru ve uygun olmasını sağlayacaktır. Süreci Okul İnternet Sitesi Yayın Ekibi ile birlikte yürütecektir.

Okul İnternet Sitesinde, erişilebilirlik, fikri mülkiyet haklarına saygı, gizlilik politikaları ve telif hakkı da dâhil olmak üzere okulun yayın yönergelerine uyulacaktır.

Öğrencilerin okulun kültürel, sosyal, sportif vb. eğitim-öğretim faaliyetlerinde yaptığı çalışmalar ve bu çalışmalara ait öğrenci fotoğrafları okulun panolarında ve okul internet sitesinde yayınlanacaktır.

Öğrenci fotoğrafları profil oluşturacak nitelikte olmayacak şekilde yayınlanır. İlgili izin veli-okul sözleşmesiyle birlikte okul idaresince veliden alınacaktır.

Spam maillerden korunmak için okul e-posta adresi çevrimiçi olarak dikkatli bir şekilde yayınlanacaktır.

Okul internet sitesinin yönetici hesabına giriş yaparken kullanılan parola-şifreler güçlü parola oluşturma kurallarına uygun bir şekilde oluşturulacaktır. İlgili yönetim paneline bakanlık Mebbis sistemi kişisel parolalarıyla girildiği için yönetim paneli için yetki verilen kişiler Mebbis kişisel parolalarının güvenliği hususuna özen göstereceklerdir.

Okul, çevrimiçi güvenlik dâhil olmak üzere, toplumu da bilinçlendirecek şekilde okul internet sitesinde dijital korunma hakkında bilgilendirmeler paylaşacaktır.

Okuldan erişim izni olan, yeni açılan bazı web sayfalarının olumsuz içerikler sunmaları durumunda özellikle okullara, öğrencilerine ve çalışanlarına zarar verebileceklerinden, dolayı bu siteler periyodik olarak izlenir. Zarar veren içerikler fark edildiği anda erişim kapatılır/kaldırılır.

3. Uygulama

eSafety Yönetimi

Okulumuzda internetin, bilgisayarların, etkileşimli tahtaların ve tüm BT araçlarının; ülkemiz anayasası, kanunlarımız ve bakanlığımız mevzuatı çerçevesinde eğitim-öğretim merkezli kullanılması esastır.

Kurum kültürümüz açısından insani, milli, manevi ve ahlaki değerlerimizi hayati derecede önemsiyoruz. İnternet ve BT araçları kullanımında tüm paydaşlarımız bilişim etiği çerçevesinde hareket etmelidir.

Okulumuzda ders anlatımı yapılan her alanda güvenli internet erişim ağı vardır. Ders anlatımlarında EBA eğitim ve eTwinning portalından yararlanılmaktadır. Güvenli internet erişim ağı, ağ güvenlik filtresiyle kullanılmaktadır. Okulumuzda Fatih TTVPN fiber internet altyapısı kullanılmaktadır.

Okulumuzun internet (web) sitesi bulunmaktadır. Bu ağların üzerinde yayınlanan veriler kontrollü olarak paylaşılmaktadır.

Okul Müdürü sorumluluğunda, Baş Müdür Yardımcısı, Türk Dili ve Edebiyatı Öğretmeni, Grafik ve Tasarım alanı öğretmeninden oluşan Okul İnternet Sitesi Yayın Ekibimiz bulunmaktadır. Okul İnternet Yayın Ekibimiz, Bursa Necatibey Mesleki ve Teknik Anadolu Lisesi e-Güvenlik koordinatörlüğü görevlerini de yürütmektedir. İhtiyaç halinde bu ekipler okul müdürlüğüne genişletilebilmektedir.

Bilgisayarlar ve Akıllı Tahtalarda lisanslı, açık kaynak kodlu veya ücretsiz ve güvenilir yazılımlar yüküdür. BT araçları okul idaresi ve öğretmenlerin kontrolünde kullanılmaktadır.

Rehberlik servisi tarafından düzenli olarak, teknoloji bağımlılığı, BT'nin doğru ve güvenli kullanımı, Siber Zorbalık gibi konularda seminerler düzenlenmektedir.

Okulumuzda BT'nin doğru ve güvenli kullanımı ile ilgili panolar hazırlanmaktadır.

Okulumuzun öğretmenleri Millî Eğitim Bakanlığı tarafından verilen Siber Zorbalık, BT'nin doğru ve güvenli kullanımı konularında uzaktan ve yüz yüze eğitimler almıştır/alacaktır.

Okulumuzda "Güvenli İnternet Günü" kutlanmaktadır.

Okulumuzun internet sitesinde e-Güvenlik konusunda, guvenliweb.org.tr gibi güvenilir sitelerden alıntılanan uyarıcı bilgiler yer almaktadır.

Okul paydaşlarımız istedikleri zaman e-güvenlik vb. konularla ilgili bilgi alabilmekteler.

Okulumuzda güvenli internet günü kutlamalarında veya konu ile ilgili seminerlerde guvenliweb.org.tr gibi güvenilir sitelerden alıntılanan bilgi broşürleri dağıtılmaktadır.

Okulumuzda 21. yüzyıl iletişim becerileri önemsenmektedir. Bununla ilgili olarak öğrencilerimizin BT kullanım becerilerini geliştirme çalışmaları yapılmaktadır.

Okulumuzda okul idaresinden izinsiz fotoğraf çekmek kesinlikle yasaktır.

Öğrencilerimizin ve velilerimizin okulumuza kayıt olurken sağladıkları kişisel bilgileri idare sorumluluğunda ve idare tarafından korunmaktadır.

Velilerimizin iletişim bilgileri kendi bilgi ve istekleri haricinde asla üçüncü şahıslarla paylaşılmaz.

Müfredatta eSafety

Okulunuzda siber zorbalık, müfredatta genç yaştaki öğrencilerle tartışılır.

Çocuk koruma politikanız dâhilinde cinselliğe özel bir atıfta bulunuruz. Çünkü bu, birçok genç insanın uğraşmak zorunda olduğu büyüyen bir konudur. Bu konuda öğrenciler için uygun bir eğitim sağlıyoruz.

Okulumuzda tüm yıl personele ve öğrencilere eSafety hakkında bilgilendirilmesi yapılır. Sürekli değişen ihtiyaçları karşıladığından emin olmak için müfredatın düzenli olarak gözden geçirilmesi önemini sürdürmektedir. Okul politikaları açıkça eSafety müfredat entegrasyonu, tüm öğretmenler tarafından yapılır. Herkes ortak sorumluluklarının bilincindedir.

Müfredat Dışı Etkinlikler

Öğrencilere, istendiğinde müfredat süresi dışında eSafety desteği sağlanır. Öğrencilere okul dışında çevrimiçi teknolojiyi kullanmaları hakkında mutlaka eğitim verilmelidir. Okul dışında gerçekleşen çevrimiçi sorunların kaçınılmaz olarak okul içinde bir etkisi olur. Bir okulun başa çıkabileceği en yaygın sorunlar, hesapların hacklenmesi, gizliliğin ihlali, cinsel içerikli mesajlaşma, aşırı kullanım ve siber zorbalıktır. Bu tür olaylara karşı öğrencilerimizin korunması önemlidir. Okul dışında meydana gelen sorunlardan okul haberdar edilir. Yasalara göre sorumlu kişilere gerekli ceza ve yaptırım uygulanması sağlanır.

Öğrencileri, zorbalık ve gizlilik ihlali gibi çevrimiçi sorunların olası sonuçları hakkında bilgilendirmek için okulda farkındalık etkinlikleri düzenlenir. Müfredat süresi dışında ne tür ek e-Güvenlik desteğinden yararlanacaklarını görmek için öğrencilerden geri bildirim alınır. Öğrencilerin çevrimiçi sorunlarla karşılaştıklarında, okul dışında veya içinde olup olmadıklarına bakılmaksızın danışabilecekleri bir öğretmen veya danışman atanmıştır. Bu kişi temel teknik tavsiyelerde bulunabilir. Sosyal Medya hesapları hakkında bilgi verilir. Siber zorbalık durumunda psikolojik tavsiyeler alabilir. Gerektiğinde, okulumuz bir konuyla ilgili tüm öğrencilerin ebeveynlerine başvurur ve gerekirse harici profesyonel yardım alması konusunda yönlendirir.

Personele çevrimiçi sorunlarla nasıl daha iyi başa çıkılabileceği konusunda yıllık eğitim düzenlenir. Öğrencilerin yaşadığı problemler raporlanır. Raporların sayısı ve niteliği takip edilir. Okulumuzdaki özel ihtiyaçlar belirlenir. Ciddi problemlerde, okul yönetimi- öğretmenler velileri telefonla arayarak bildirir. Okul Yönetimi ve Rehberlik Servisi incelemesi sonunda öğrencileri psiko-eğitimi okulda ya

da özel destek almaları konusunda yönlendirir.

Destek Kaynakları

- Tüm personelin eSafety için bir sorumluluğu olmalıdır. Okul rehber öğretmenleri e-Güvenlik konularında tavsiye ve rehberlik sağlamak için iyi bir konumdadır. Okul Politikanızı geliştirmeye ve düzenli olarak gözden geçirmeye katkıda bulunmak için okuldaki diğer personeller toplantılara davet edilir.
- Okulumuzdaki öğrenciler aktif olarak eSafety montörü olmaları için teşvik edilir. eSafety Label ağının geliştirilmesi için eSafety içerikleri, web sayfamızda paylaşılır. Okul Panolarında eSafety Label logosuna yer verilir. Görünürlüğü sağlanır.

Personel Eğitimi

eSafety konularında ortaya çıkan trendler hakkında tüm personelin düzenli olarak bilgilerinin güncellenir. Okuldaki tüm personelin <https://www.esafetylevel.eu/group/community> adresine üye olmaları istenir. Bu sitede paylaşımda bulunmaları ve e-Güvenlik konusunda destek alacakları açıklanır. Personelin eğitimlerinde neye ihtiyaçları olduğunu belirlemek için mutlaka bir ihtiyaç analizi yapılır. Anket yapılır. Anket sonuçları Kaynaklar bölümüne yüklenir. Forum bölümünde, üye öğretmenlerle değerlendirilir.

Okulumuzda personel üyeleri arasındaki bilgi alışverişi teşvik edilir. Bu, tüm okul için faydalı olacaktır. “Okul alanım” aracılığıyla da erişilebilen yükleme aracı aracılığıyla eSafety konularında belgeler yüklenir.

Yararlı Linkler

- 1.eSafety Label
<https://www.esafetylevel.eu/>
- 2.eSafety Label Hakkında Her Şey
<https://etwinningonline.eba.gov.tr/course/esafety-label-hakkinda-hersey/>
- 4.İnternet Güvenliği ve eTwinning Etiği
<https://etwinningonline.eba.gov.tr/course/internet-guvenligi-ve-etwinning-etigi/>
- 5.E güvenlik test - Öğretim kaynakları – Wordwall
<https://wordwall.net/tr-tr/community/e-g%C3%BCvenlik-test>
- 6.Interland - Be Internet Awesome
https://beinternetawesome.withgoogle.com/tr_all/interland
- 7.Güvenli Çocuk
<https://www.guvenlicocuk.org.tr/>
- 8.Eba Siber Güvenlik Portalı
<https://www.eba.gov.tr/siber-guvenlik>
- 9.Siberay
<https://www.siberay.com/>
- 10.İnternet Etiği
<https://www.guvenliweb.org.tr/dokuman-detay/internet-etigi>
- 11.MEB Bilgi ve Sistem Güvenliği
<http://mevzuat.meb.gov.tr/dosyalar/1955.pdf>
- 12.AB Genel Veri Koruma Yönetmeliği GDPR
<https://www.kisiselverilerinkorunmasi.org/wp-content/uploads/2017/09/GDPR-T%C3%BCrk%C3%A7e-%C3%87eviri-AB-Bakanl%C4%B1%C4%9F%C4%B1.pdf>
- 13.İnterneti Nasıl Kullanmalıyım
https://orgm.meb.gov.tr/meb_iys_dosyalar/2020_11/13160844_LIYSE_OYGYRENCIY.pdf
- 14.Bilinçli İnternet Kullanımı
<https://orgm.meb.gov.tr/www/bilincli-internet-kullanimi-e-brosurleri-yayinlandi/icerik/1500>
- 15.Güvenli İnternet Kullanımı

https://orgm.meb.gov.tr/meb_iys_dosyalar/2019_12/26113028_GUVENLY_YNTERNET_KULLANI_ML.pdf

16.Siber Zorbalık

<https://orgm.meb.gov.tr/www/siber-zorbalik/icerik/2086>

17.Okullarda Sosyal Medyanın Kullanılması

<http://mevzuat.meb.gov.tr/dosyalar/1833.pdf>

18.Fikir Ve Sanat Eserleri Kanunu

<https://www.mevzuat.gov.tr/mevzuatmetin/1.3.5846.pdf>

Okul e-Twinning Komisyonu

Nademin ŞAHİN

Birsen YAŞBEK

Tülay GÜRDAL

Eda AKÇAMLI

Serap BİRCAN

Burcu ÖZTÜRK

Dilara SEVİNÇ

Serpil ÇAKMAK

