KABUL EDİLEBİLİR KULLANIM POLİTİKASI
BİLGİLENDİRME METNİ

1. AMAÇ

Bu politikanın amacı, Namık Kemal Ortaokulu Bilgisayar Sistemlerinin kullanım koşullarını ve kabul edilebilir kullanım politikasını belirlemektir.

- Politikamız; yöneticiler, öğretmenler, diğer çalışanlar, öğrenciler ve veliler için hazırlanmış olup, kişilerin internet erişimi ve bilgi iletişim cihazlarını kullanımında çevrimiçi olarak korunmasını ve güvenliğini sağlamak.
- Teknolojinin potansiyel yararları, etkileri ve riskleri konusunda Namık Kemal Ortaokulu yöneticileri, öğretmenleri, öğrencileri, velileri ve çalışanları için farkındalık yaratmak.
- Tüm personelin güvenli ve sorumlu bir şekilde çalışmasını sağlamak, olumlu davranışları modellemek, teknolojiyi kullanırken kendi standartlarını ve uygulamalarını yönetme gereksiniminin farkında olmak.
- Okuldaki tüm üyeler tarafından bilinen çevrimiçi güvenlik endişelerine yanıt verirken açıkça kullanılacak prosedürleri tanımlamak.
- Bu politikanın, yöneticiler, öğretmenler, öğrenciler, veliler, destek personeli, harici yükleniciler, ziyaretçiler, gönüllüler ve okul adına hizmet veren veya bunları yerine getiren diğer kişiler (toplu olarak bu politikada ´personel´ olarak anılacaktır) dahil olmak üzere tüm personel için geçerli olmasını sağlamak.

Sonuç olarak ana hedefimiz, internet erişimi ve kişisel cihazlar da dahil olmak üzere bilgi iletişim cihazlarının kullanımı için bu güvenlik politikasının geçerli olmasıdır. Öğrenciler, personel ya da diğer kişilere, çalıştıkları dizüstü bilgisayarlar, tabletler veya mobil cihazlar gibi uzaktan kullanım için okul tarafından verilen cihazlar için de geçerlidir.

2. KAPSAM

Bu politika, tüm Namık Kemal Ortaokulu Bilgisayar Sistemleri ve Bilgi Teknoloji servislerine okul içinden veya dışından erişim hakkı verilen tüm kullanıcıları kapsar.

3. TANIMLAR

Bilgisayar Sistemleri

Bilgisayar sistemleri her türlü bilgisayar ile ilgili donanım, teçhizat ve fikri mülkiyeti ifade eder. Buna, okulun sahip olduğu, kiraladığı, uyarladığı veya okulun sahipliğinde bulundurduğu, muhafaza altına aldığı veya kontrolü altında olan bilgisayar sistemleri, kişisel bilgisayarlar, mobil cihazlar, bilgisayar ağları ve her türlü yazılım, donanım yazılımı, işletim yazılımı ve uygulama yazılımı dâhildir. Açık olmak adına, "bilgisayar sistemleri" okul tarafından uyarlanan yerel ağ, bulut veya internet temelli hizmetleri veya okul faaliyetlerinin veya okul verisinin saklanmasında kullanılan genel nitelikli yerel ağ, yürütülmesinde bulut veya internet temelli hizmetleri kapsar.

Kötü amaçlı yazılım

Kötü amaçlı yazılım, meşru bir kullanıcının bilgisayarına virüs bulaştırmak ve birkaç yolla zararı artırmak için tasarlanan bir tür bilgisayar programıdır. Kötü amaçlı yazılım, bilgisayarlara ve cihazlara birkaç biçimde virüs bulaştırabilir ve çeşitli türleri vardır. Bunlardan birkaçı virüsler, solucanlar, Trojanlar, casus yazılımlar ve diğerleridir.

4. TEMEL PRENSİPLER

Kullanım Koşulları

Tüm kullanıcılar; okulun bilgisayar sistemlerini kullanarak, okulun söz konusu sistemlerde saklanan veya bu sistemler aracılığıyla gönderilen hiçbir ileti veya verinin gizliliği hakkında herhangi bir beyanda bulunmadığını; okulun bu dokümanda belirtilen haklarını saklı tuttuğunu ve söz konusu sistemlerin kullanımının okul onaylı amaçlar ile sınırlı olduğunu, bu hususta kendilerine gerekli bildirimlerin yapılmış olduğunu kabul ederler.

Okulun bilgisayar sistemlerinin okul faaliyetleri ve önem arz etmeyen konulardaki kişisel kullanımı ile ilişkili olarak kullanılması bir hak değil ancak okul topluluğunun sınırlı üyelerine tanınan bir ayrıcalıktır. Dolayısıyla, okul dilediği zaman ve herhangi bir bildirimde bulunmaksızın bilgisayar sistemlerinin tamamına veya bir kısmına erişimi (tüm kullanıcılar veya bazı kullanıcılar için) tamamen veya kısmen engelleyebilir. Okulun bilgisayar sistemleri kullanıcıları, işbu Namık Kemal Ortaokulu "Kabul Edilebilir Kullanım Politikası"na uymak zorundadır ve söz konusu sistemleri kullanarak "Kabul Edilebilir Kullanım Politikası"nı kabul etmiş olduklarını ve bunlara uyacaklarını, bu hususta kendilerine bildirim yapılmış olduğunu ve okulun "Kabul Edilebilir Kullanım Politikası"nı uygulamasına izin vermiş olduklarını kabul etmiş olurlar.

Kullanıcılar aynı zamanda ilgili mevzuata uyacaklarını ve okulu yükümlülük altına sokacak her türlü davranıştan kaçınacaklarını kabul ederler. Okul, işbu Namık Kemal Ortaokulu "Kabul Edilebilir Kullanım Politikası" ile bilgisayar sistemlerinin kullanımına ilişkin diğer koşulları dilediği zaman önceden herhangi bir bildirimde bulunmaksızın değiştirme hakkını ve ilgili mevzuat gereğince alınması gereken veya alınması uygun olan aksiyonları alma hakkını saklı tutar.

Okul, okulun bilgisayar sistemleri ile kullanıcılarının bütünlüğünün söz konusu tesislerin yetkisiz veya uygunsuz kullanımına karşı korunması ve okulun kural ve politikalarının ihlali veya ihlaline neden olacak muhtemel kullanımların tespiti için; herhangi bir bildirimde bulunmaksızın herhangi bir kişinin kullanımını sınırlama veya engelleme ve bir bilgisayar sistemleri için uygun görülen kullanımı zedeleyecek ya da okulun kural veya politikalarının ihlali için kullanılabilecek olan her türlü veri, dosya veya sistem kaynağını araştırma, kopyalama, kaldırma veya değiştirme hakkını saklı tutar.

Namık Kemal Ortaokulu bilgisayar sistemlerinin korunması için sistemlerin periyodik kontrolüne ilişkin hakları ve diğer her türlü hakkını saklı tutar. Okula ait bilgisayarlarda, akıllı tahtada, sunucularda, okul sunucularında işlenen e-posta mesajlarında zararlı yazılım taraması sistemleri koruma amaçlı yapılacak kontrollere örnektir.

Okul, söz konusu sistemlerin gizlilik ve güvenliğinin sağlanması için gerçekleştireceği çalışmalardan, sistem bozukluğundan veya diğer bir sebepten meydana gelecek veri kaybından veya dosyalara müdahale edilmesinden sorumlu değildir.

• E-GÜVENLİK POLİTİKAMIZ:

Dijital teknolojiler okul çağı çocukları için de olağanüstü imkanlar ve fırsatlar sunuyor. Çocuklar da internet ortamının sağladıklarıyla bilgiye, eğlenceli oyunlara ve benzeri etkinliklere kolayca ve hızlıca erişim sağlayabiliyorlar. Ancak, dijital teknolojilerin sağladığı bu harika imkanların yanında, çocuğun zihinsel, ruhsal ve fiziksel saldırılarla, tuzaklarla karşılaşması tehlikesinin varlığı da hafife alınamaz bir gerçekliktir. Güvenli bir ortam sağlamak için, risklerin çeşitlerini, sıklığını ve bunları azaltmak veya daha da iyisi ortadan kaldırmak için çözümleri üretmemiz gerekir.

Örnek vermek gerekirse internet ortamındaki bir çocuğun istem dışı da olsa karşısına çıkan bir reklamı izleme yoluyla ya da arama motoruna bilerek-bilmeyerek yazacağı yanlış bir kelime sebebiyle pornografik bir siteye girmesi mümkündür ya da çocuğun merakını kışkırtan bir görsel onu zihinsel, duygusal ve fiziksel olarak tehlikeye düşürecek ortamlara sürükleyebilir.

Çevrimiçi öğrencilerin karşılaştığı risklerden biri de siber zorbalık veya çevrimiçi mağduriyettir: yani elektronik iletişim şekillerini kullanan zorbalık veya taciz. Siber zorbalığın bazı örnekleri açıkça tanımlanabilirken diğerleri daha azdır. Siber kelimenin mağdurunu korkutmak için kullandığı dil ve taktiklerin cezai bir suç olduğunun açık işareti olduğu durumlarda olabilir, bazı durumlarda ise yalnızca bir şahsın kötü davranışlarından kaynaklanır. Siber zorbalık, genellikle eylemin tekrarını gerektirir.

İnternetteki siber zorbalığa hitap etmenin bir yolu, okul zorbalığı ve siber zorbalık arasındaki bağlantıyı kullanmaktır. Okul zorbalığına, öğrencilerin sahip oldukları ve birbirlerine karşı olan ilişkileri ve tutumları geliştirmeye çalışan girişimler denir. Bu tür girişimleri, çevrimdışı zorbalığa karşı koymak için potansiyel olarak etkili önleme tedbirleri olarak düşünülmekte ve çevrimiçi zorbalığa karşı koymada da yararlı olabilirler.

Öğrenciler ve yetişkinler genellikle çevrimiçi mağduriyet konusunda farklı yorumlara sahiptir. Yetişkinler bazı eylemleri bir şekilde tedavi etme eğilimi gösterirken, öğrenciler aynı örnekleri akranları arasında normal bir etkinlik olarak açıklayabilir, ancak bunlar çevrimdışı bir sorunla başlar.

Okulumuz, okul çapında bir zorbalık önleme programının oluşturulmasını kolaylaştıracak politikalar oluşturur ve bu programlar tipik olarak etkinliklerinin periyodik değerlendirmelerini içerir. Başarılı ve etkili programlar, bireysel öğrencilerden ve sınıflardan, eğitimcileri ve öğrencileri birleştiren zorbalık karşıtı takımlara kadar, okulda her seviyede zorbalık karşıtı stratejileri teşvik etmek için çalışır.

Ağır internet kullanıcıları uygunsuz içerikle çevrimiçi karşılaşabilir; öğrenciler genellikle cinsel taciz veya cinsel içeriğe online olarak maruz kalma ile karşı karşıya kalabilir. World Wide Web'deki sınırsız içerik, olgunlaşmamış gençleri istenmeyen cinsel içeriğin ve bilginin geniş bir koleksiyonuna götürebilir. Örnekler, cinsel ilişki talepleri, cinsel konuşmalar, cinsel fotoğraflar gönderme veya talep etme veya istenmeyen cinsel bilgilerin ifşa edilmesini içerir. Ayrıca, istenmeyen pop-up'lar vasıtasıyla cinsel olmayan içerik için web'de gezinirken, öğrenciler bazen müstehcen içerik veya cinsel fotoğraflarla/ videolarla karşı karşıya kalırlar. E-posta dolandırıcılıkları alabilirler.

Çoğu öğrenci, utanç yüzünden çevrimiçi olarak karşılaştıklarında yetişkinleri dahil etmeme eğiliminde oldukları için, ebeveynlerin ve eğitimcilerin, öğrencilerin zorluklarla karşılaşabileceğini belirtmek için dikkat etmeleri gereken işaretlerden haberdar edilmesi gerekir.

Bu nedenle, okulumuzda uzman kişiler tarafından; personele, öğrencilere ve ebeveynlere eğitimler/seminerler organize edilirken, diğer etkin yöntemler olarak, filtreleme ve güvenlik duvarı teknolojilerini kullanmakta ve tavsiye etmekteyiz.

Öğrencilerin daha proaktif olarak çevrimiçi mahremiyetlerini korumaları durumunda, internetin oluşturduğu risklerin birçoğu azaltılabilir. Kişisel bilgilerin çevrimiçi olarak açığa çıkmasına daha az istekli olacak şekilde eğitilmeleri ve gizliliklerini nasıl yöneteceklerini bilmeleri gerekir; Bu tür eğitim, özellikle genç yaştan itibaren okullarda önemlidir. Ebeveynler ve çocukları arasındaki nesil boşluğu nedeniyle, birbirlerine güven duymalarını engelleyebilecek ve dolayısıyla çevrimiçi riskin etkili bir şekilde kontrol altına alınmasına neden olabilecek bir yanlış anlama olasılığı bulunmaktadır.

Yukarıda kısaca söz edilmiş olan tehlikelerden çocuğu korumanın en emin yolu, onu internet ortamından tamamen uzak tutmaktır. Ancak çok hızlı gelişen dijital teknolojiler sebebiyle ve ne yazık ki, çocuğu internet ortamından tamamen uzak tutmak mümkün olmamakta, tamamen yasaklamak sorunu çözmemektedir. Kaldı ki çevresel etkenler ve ebeveyn tutumları sebebiyle internet ortamlarını tamamen yasaklamak ve erişimi engellemek imkansız bir hal almıştır. Bu sebeple çocuğu internet ortamının oluşturduğu tehlikelerden korumak için tamamen yasaklamaya çalışmaktan daha etkili tedbirler bulmak zorunluluğu vardır.

Öncelikle ifade etmek gerekir ki, dijital teknolojilerin sahip olduğu imkanlar sebebiyle alınabilecek hiç tedbir çocuğu yukarıda sözü edilen tehlikelerden yüzde yüz oranında koruyamayacaktır.

Bu nedenle, okulumuzda öğrencilerle yetişkinler arasındaki iletişim teşvik edilmektedir. Siber güvenlikle ilgili diyaloga girmek, boşluğu hafifletmeye ve güvenlik tedbirlerini geliştirmeye yardımcı

olabilir. Bu tür diyaloglar aynı zamanda öğrencileri, ebeveynlerini çevrimiçi olan kaynaklar ve web siteleri konusunda eğitmeye teşvik edebilir.

Dolayısıyla söz konusu tehlikelerden kendisini koruması için çocuğa bilgi, bilinç ve davranış kazandırmaktan, bu hedef için çaba harcamaktan daha etkili bir yol kalmamaktadır.

Bu gerçekler sebebiyle; okul politikası olarak, öğrencilerimizi internet ortamlarının tehlikelerinden ve zararlarından koruyabilmek için ısrarlı ve kararlı bir şekilde uygulamalar gerçekleştirir.

Çocuklarımızın dijital teknolojiler aracılığıyla; sunulan fırsatlardan en iyi şekilde, nasıl yararlanacaklarını bilmelerini sağlamak için, bunları nasıl kullanacaklarını bilmeleri ve anlamaları gerekiyor. Bunun evde, okulda veya dışarıda, arkadaşlarla veya yalnızken yapılmasını sağlamak için okulumuzun açık ve öz bir okul politikası hazırlanmıştır.

Güvenlik okuldaki her öğretmenin sorumluluğundadır. Ancak okul e-Güvenlik politikasının uygulanmasından okul müdürü, gözden geçirilmesinden ve eyleminden okul e-Güvenlik koordinatörü sorumlu olup; e-Güvenlik komisyonuna ve okul müdürüne en az yılda iki kez veya eğitimin kullanımındaki önemli yeni gelişmeler ışığında düzenli olarak rapor verecektir. E-Güvenlik koordinatörü Eylül ayının ilk haftasında öğretmen kurul toplantısında seçilir. (Genellikle Bilişim Teknolojileri öğretmeni yoksa müdür yardımcısı seçilir.)

Okul e-Güvenlik Politikamız; personelin, öğrencilerin ve ebeveynlerin güvenliği ile okulun itibarı ve geleceğiyle ilgili dijital gelişmelere ve yeni eğilimlere ayak uydurmaktadır.

Amaca uygun okul e-Güvenlik Politikası, AUP ve okuldaki diğer güvenlikle ilgili politikalarla uyumludur.

Okul e-Güvenlik Politikası oluşturulurken paydaşların(öğrenciler, personel, ebeveynler ve daha geniş topluluk üyeleri.) politikanın belirli bölümlerine sahip olması ve dolayısıyla politikaya uyma olasılıklarının daha yüksek olması için katılımı sağlanmaktadır.

Okul e-Güvenliği politikası, tüm personelin ve öğrencilerin kendilerinden ne beklendiğini bilmelerini sağlayan açık yönergelerle, anlaşılması kolay, teknik olmayan bir dildedir.

- Öğrencilerimiz farklı ekonomik koşullara ve şartlara sahip ailelerin çocuklarıdır. Okulumuzda her sınıfta akıllı tahta vardır. Tahtalar için her öğretmende anahtar bulunmaktadır. Bir Bilişim okul formatörümüz bulunmaktadır. Okulumuzda; 21 şube vardır. Okulumuzda ders anlatımı yapılan her alanda güvenli internet erişim ağı vardır. Ders anlatımlarında EBA eğitim ve eTwinning portallerinden de yararlanılmaktadır. Güvenli internet erişim ağı, ağ güvenlik filtresiyle kullanılmaktadır.
- Okulumuzda eTwinning portaline üye olmuş; 2018 yılından beri "Güvenli İnternet Günü" kutlanmaktadır. Bütün yapılan projelerin içine kutlama etkinliği olarak konulup, öğrencilerimiz tarafından kutlanmaktadır. Ve yapılan çalışmalar sürekli olarak panoda sergilenmektedir. Ayrıca okulumuzda güvenli internet günü kutlamalarında, konu ile ilgili seminerlerde www.guvenliweb.org.tr sitesinden alıntılanan bilgi broşürleri dağıtılmaktadır.
- Okulumuzda 21.yy iletişim becerileri önemsenmektedir. Bununla ilgili olarak öğrencilerimizin BİT kullanım becerilerini geliştirme çalışılmaları yapılmaktadır.
- Okul paydaşlarımız istedikleri zaman konu ile ilgili bilgi alabilmekteler.
- Okulumuzda Dijital vatandaş olma(dijital okur-yazarlık, dijital ayak izi, bulut…) konusunda paydaşlarımızı bilinçlendirme çalışmaları yapılmaktadır.
- Okulumuzda izinsiz fotoğraf çekmek kesinlikle yasaktır. Etkinliklerde yer alacak öğrenciler izin veli izin dilekçesi talep edilecektir. Okulumuzun öğrencilerinin yüzleri okula ait hiçbir sosyal medya sitesinde ve eTwinning portalı dahilindeki proje resimlerinde açık bir şekilde gösterilmeyecektir. Yüzü gözükme durumu olan personele bilgi verilerek; kabul ettiğini ve istediği zaman cayma hakkını belirten dilekçe alınacaktır. Kabul etmiyorsa kişinin görseli ya da şahsına ait belge paylaşılmayacaktır.

A) HAKLAR VE SORUMLULUKLAR

-Bu politikanın uygulatılmasından yönetim sorumludur.
-Bu politikanın hazırlanmasından e-Güvenlik Komisyonu, güncellenmesinden e-Güvenlik koordinatörü sorumludur.

1) OGYE EKİBİ

Unvanı	Ekipteki Görevi	Adı Soyadı
Müdür Başyardımcısı	Başkan	Bülent Vural SAVAŞ
Sosyal Bilgiler Öğretmeni	Üye	Deniz YAPICI
Matematik Öğretmeni	Üye	Elif GÖKTEPE
İngilizce Öğretmeni	Üye	Yeşim YILMAZ

2) YÖNETİM VE OGYE E-GÜVENLİK DEĞERLENDİRMESİ

Okul yönetimi, Okul Gelişim ve Yönetim Ekibi ile bir araya gelerek okulun bilgi ve iletişim sistemlerinin kullanımının nasıl olduğu ve nasıl olması gerektiği üzerine görüş belirterek; durum değerlendirmesi yaptılar. Yapılacak olan çalışmaları belirlediler.
Yapılacak çalışmalarda;
-eGüvenlik Koordinatörü tarafından bilinçli ve güvenli internet kullanımı üzerine öğrencilere, velilere ve personele seminerler verilecektir.
-eGüvenlik panosundaki uyarılar ve bilgilendirmeler güncellenecektir.
-eGüvenlik ile ilgili seminerlerle ilgili afişlerin web sitesinde yayınlanacaktır.
-eGüvenlik ile ilgili bilgilendirme dokümanlarının okul web sitesinde yayınlanmasına devam edilecektir.

3) STRATEJİK PLANIMIZDA E-GÜVENLİK

2019-2023 dönemi Stratejik Planımızda eGüvenlik ile Teknoloji konularına atıfta bulunulmuştu. Varolan planımızın amaç,hedef ve eylemleri ile misyonumuzda bu konular üzerinde durulmuştur. SWOT analizlerimiz yapılırken yine güçlü ve güçsüz yönlerimizde durum değerlendirmeleri yapılmıştır. Okulumuzun web sitesinde güncel hali mevuttur.

3.1.STRATEJİK PLAN ÜST KURULU VE STRATEJİK PLANLAMA EKİBİ

ÜST KURUL BİLGİLERİ		**EKİP BİLGİLERİ**	
Adı Soyadı	**Unvanı**	**Adı Soyadı**	**Unvanı**
Mehmet Fahri ASLAN	Okul Müdürü	Bülent Vural SAVAŞ	Müdür Yardımcısı
Seval İŞLEK	Rehber Öğretmen	Seval KAVALCI	Türkçe Öğretmeni
Merve TEMELLİ	Bilişim Öğretmeni	Begüm ÖZCAN YAVUZ	Matematik Öğretmeni
İrem ERSÖZ	Okul Aile Birliği Başkanı	Şerife Demir KAYMAK	Fen Bilimleri Öğretmeni
İlkay ÖZCAN	Okul Aile Birliği Üye	Ömer ALEMDAR	Beden Eğitimi Öğt.
		Dicle ÇELİK	Sosyal Bilgiler Öğrt.
		Songül ERSÖZ	Veli

3.2. STRATEJİK PLANIMIZDAKİ TEKNOLOJİK KAYNAKLAR TABLOSU

Akıllı Tahta Sayısı	22	TV Sayısı	1
Masaüstü Bilgisayar Sayısı	6	Yazıcı Sayısı	4
Taşınabilir Bilgisayar Sayısı	1	Fotokopi Makinası Sayısı	3
Projeksiyon Sayısı	1	İnternet Bağlantı Hızı	16
Kamera sistemi	1	Kamera sayısı	12

3.3.GZFT (GÜÇLÜ, ZAYIF, FIRSAT, TEHDİT) ANALİZİ

Okulumuzun temel istatistiklerinde verilen okul künyesi, çalışan bilgileri, bina bilgileri, teknolojik kaynak bilgileri ve gelir gider bilgileri ile paydaş anketleri sonucunda ortaya çıkan sorun ve gelişime açık alanlar iç ve dış faktör olarak değerlendirilerek GZFT tablosunda belirtilmiştir. Dolayısıyla olguyu belirten istatistikler ile algıyı ölçen anketlerden çıkan sonuçlar tek bir analizde birleştirilmiştir.

Kurumun güçlü ve zayıf yönleri donanım, malzeme, çalışan, iş yapma becerisi, kurumsal iletişim gibi çok çeşitli alanlarda kendisinden kaynaklı olan güçlülükleri ve zayıflıkları ifade etmektedir ve ayrımda temel olarak okul müdürü/müdürlüğü kapsamından bakılarak iç faktör ve dış faktör ayrımı yapılmıştır.

İÇSEL FAKTÖRLER

Güçlü Yönler

Öğrenciler	Farklı durumlarda olmalarına rağmen farklı alanlarda yetenekleri olan öğrencilerimiz bulunmaktadır.
Çalışanlar	Eğitim kadrosu arasında dayanışma ve işbirliğinin kuvvetli olması
Veliler	Sayı azlığından dolayı erişimin kolay olması
Bina ve Yerleşke	Çarşı merkezinde ulaşılabilir olması
Donanım	Okulumuzun teknik araç ve gereç ve yeterli donanıma sahip olması
Bütçe	Öğrenci ve veli bağışları bulunmaktadır.
Yönetim Süreçleri	Yönetim ve personel arasındaki iletişimin kuvvetli olması
İletişim Süreçleri	Sorun çözmede öğretmenlerin ve idarenin destek olması.

Zayıf Yönler

Öğrenciler	Ekonomik yönden zayıf durumda olan öğrenci sayısının fazla olması
Çalışanlar	Okul bahçe ve bina alanının büyük olmasından dolayı işlerin aksatılabilmesi, kadrolu çalışan olmaması.
Veliler	Öğrencileri ile yeterince ilgili olmaması.
Bina ve Yerleşke	Çarşı merkezinde olması yüzünden trafik güvenliği olmaması, park alanı sorunu.
Donanım	Kütüphane, laboratuvar alanların sınıfa çevrilmiş olması.
Bütçe	Velilerimizin ilgisizliğinden dolayı bağış ve sosyal etkinliklerden gelirimiz bulunmamaktadır.
Yönetim Süreçleri	Müdür yardımcısı normunun bulunmasına rağmen mevcut müdür yardımcısı bulunmamasıdır.
İletişim Süreçleri	Yoktur.

DIŞSAL FAKTÖRLER

Fırsatlar

Politik	Liselere geçişte adrese dayalı sistem dışında istedikleri okula kayıt yaptırabilmeleri
Ekonomik	Okulumuzda ihtiyacı olan öğrencilere örnek kitaplar verilmesi.
Sosyolojik	Çeşitli yarışmalarda öğrencilerimizin katkı sağlaması
Teknolojik	Bilişim formatörümüz bulunmaktadır.
Mevzuat-Yasal	Sınıflarda bir durum oluştuğunda disiplin kurulu işler hale gelebiliyor.
Ekolojik	-

Tehditler

Politik	-
Ekonomik	Düşük gelirli ailelerin çoğunluktaolması
Sosyolojik	Öğrencilerin okul sonrası yaşamlarında yeterince sosyal ortamlarda bulundurulmaması
Teknolojik	Her öğrencide hemen hemen telefon olması
Mevzuat-Yasal	Ortaokulda disiplin kurulu caydırıcılığı yoktur.
Ekolojik	Bulunduğumuz konumdan dolayı kötü hava şartlarında okulumuz bahçesi olumsuz etkilenmektedir.

3.4.GELİŞİM VE SORUN ALANLARIMIZ

2.TEMA: EĞİTİM VE ÖĞRETİMDE KALİTE	
1	Akademik Başarı
2	Değerler Eğitimi
3	Sosyal, Kültürel ve Fiziksel Gelişim
4	Yerel - Ulusal ve Uluslararası Projeler
5	Kurum Kültürü

Sonuç olarak 2019-2023 stratejik planımız ekip tarafından hazırlanırken; BİT ve güvenlik konuları, seminerler verilmesi ile projelerin devamlılığı gibi konular üzerinde durulmuş ve planımızda 2019 yılında yerini almıştır. Güncellemeye gerek kalmaksızın bu hali günümüz standartlarına cevap verecek niteliktedir. Yine de eğitim ve teknoloji kendini sürekli yenileyen bir döngü olduğu için, ekibimiz bir araya gelerek durum değerlendirmesi yapmıştır.

4) ÇEVRİMİÇİ HAK VE SORUMLULUĞU KAPSAYAN KONULAR

- Okul içinde ve dışında teknoloji kullanımına dair okulun belirlediği sorumlu kullanım kurallarına uymak.
- Online materyalleri kullanırken referans gösterme ve izin alarak kullanmak.
- Sınavlarda ve ödevlerde teknolojiyi kullanarak hile yapmamak.
- Siber zorbalığı, tehditleri ve diğer uygunsuz kullanımları şikayet etmek

4.1. ÇEVRİMİÇİ HAKLARIMIZIN YASAL DAYANAKLARI

- Okul e-Güvenlik Politikasında atıfta bulunulan mevzuatlar takip edilerek süreç devam ettirilir.

Personelin, öğrencilerin ve velilerin; çevrimiçi teknolojilerin sağlıklı kullanımı konusundaki farkındalığını teşvik etmek için çeşitli bilgilendirmeler ve seminerler düzenlenmektedir. Okulumuzda e-Güvenlik konusunda gerekli bütün önlemlerin alınmasının yanında, seminerlerde çeşitli siteler ya da antivirüs programları önerilerinde bulunulmaktadır.

***Code of EU Online Rights – AB Çevrimiçi Haklar Yönetmeliği https://ec.europa.eu/digital-single-market/code-eu-online-rights/ sitesinden bilgi ve yardım alabiliyoruz.

***Çevrim içi durumumuzdaki haklarımızla ilgili ülkemizde https://internet.btk.gov.tr/ sitesinden bilgi ve yardım alabiliyoruz.

***İnternet ortamında yapılan yayınların düzenlenmesi ve bu yayınlar yoluyla işlenen suçlarla mücadele edilmesi hakkında kanun
https://www.mevzuat.gov.tr/mevzuat?MevzuatNo=5651&MevzuatTur=1&MevzuatTertip=5
Kanun Numarası: 5651
Kabul Tarihi: 4/5/2007
Yayımlandığı Resmî Gazete: Tarih: 23/5/2007 Sayı: 26530
Yayımlandığı Düstur: Tertip: 5 Cilt: 46

***5651 sayılı Kanununun 8 inci maddesinde erişimi engellenebilecek suçları katalog halinde saymıştır. İnternet ortamında yapılan ve içeriği aşağıdaki suçları oluşturduğu hususunda yeterli şüphe sebebi bulunan yayınlarla ilgili olarak erişimin engellenmesine karar verilir. Bunlar:
*26/9/2004 tarihli ve 5237 sayılı Türk Ceza Kanununda yer alan;
- İntihara yönlendirme (madde 84),
- Çocukların cinsel istismarı (madde 103, birinci fıkra),
- Uyuşturucu veya uyarıcı madde kullanılmasını kolaylaştırma (madde 190),
- Sağlık için tehlikeli madde temini (madde 194),
- Müstehcenlik (madde 226)
- Fuhuş (madde 227)
- Kumar oynanması için yer ve imkân sağlama (madde 228), suçları ve
*25/7/1951 tarihli ve 5816 sayılı Atatürk Aleyhine İşlenen Suçlar Hakkında Kanunda yer alan suçlar;
Bu suçlardan bir veya birkaçına ilişkin suç tespit edilen bir internet sitesi ile ilgili vatandaşlarımız ihbarweb. org.tr adresinden şikâyetlerini gerçekleştirebilmektedirler.

***Bilişim suçlarına yönelik Türkiye'de ilk yasal metin, 765 sayılı Türk Ceza Kanununa 1991 yılında eklenen "…bilgileri otomatik işleme tabi tutan sistem…" ibaresidir. Bundan sonra ortaya çıkan ihtiyaçlar neticesince birçok kanuna bilişim ile ilgili hükümler eklenmiştir.

***Bilişim suçları ile ilgili en kapsamlı düzenleme 5237 sayılı Türk Ceza Kanununda yer almaktadır.
Türk Ceza Kanununun onuncu bölümünde bilişim alanında suçlar başlığı altında bilişim sistemine girme, sistemi engelleme, bozma, verileri yok etme veya değiştirme ile banka ve kredi kartlarının kötüye kullanılması konularında düzenleme getirmiştir.
Türk Ceza Kanununun 243. 244. ve 245. maddelerinden bilişim suçları düzenlene müstakilen düzenlenmiştir.
*Bilişim Sistemine Girme Suçu: Türk Ceza Kanununun 243. maddesi,
*Sistemi Engelleme, Bozma Verileri Yok Etme Veya Değiştirme: Türk Ceza Kanununun 244. maddesi,

*Banka Veya Kredi Kartlarının Kötüye Kullanılması: Türk Ceza Kanununun 245. Maddesi.

*** İnternet toplu kullanım sağlayıcıları hakkında yönetmelik:
https://www.mevzuat.gov.tr/mevzuat?MevzuatNo=23501&MevzuatTur=7&MevzuatTertip=5

*** internet ortamında yapılan yayınların düzenlenmesine dair usul ve esaslar hakkında yönetmelik
https://www.mevzuat.gov.tr/mevzuat?MevzuatNo=11746&MevzuatTur=7&MevzuatTertip=5

***Elektronik haberleşme sektöründe şebeke ve bilgi güvenliği yönetmeliği
https://www.mevzuat.gov.tr/mevzuat?MevzuatNo=19880&MevzuatTur=7&MevzuatTertip=5

***Mesafeli sözleşmeler yönetmeliği:
https://www.mevzuat.gov.tr/mevzuat?MevzuatNo=20237&MevzuatTur=7&MevzuatTertip=5

***İnternet alan adları yönetmeliği:
https://www.mevzuat.gov.tr/mevzuat?MevzuatNo=14416&MevzuatTur=7&MevzuatTertip=5

***Kişisel verilerin korunması kanunu
https://www.mevzuat.gov.tr/mevzuat?MevzuatNo=6698&MevzuatTur=1&MevzuatTertip=5
Kanun Numarası: 6698
Kabul Tarihi: 24/3/2016
Yayımlandığı Resmi Gazete: Tarih: 7/4/2016
Sayı: 29677
Yayımlandığı Düstur: Tertip: 5
Cilt: 57

*** Bilgi edinme hakkı kanunu:
https://www.mevzuat.gov.tr/mevzuat?MevzuatNo=4982&MevzuatTur=1&MevzuatTertip=5
Kanun Numarası: 4982
Kabul Tarihi: 9/10/2003
Yayımlandığı Resmi Gazete: Tarih: 24/10/2003
Sayı: 25269
Yayımlandığı Düstur: Tertip: 5
Cilt: 42

4.2.TÜM ÇALIŞANLARIN KİLİT SORUMLULUKLARI ŞUNLARDIR:

- ✓ Kabul Edilebilir Kullanım Politikalarını(AUP) okumak ve onlara bağlı kalmak.
- ✓ Çevrimiçi güvenlik politikalarının geliştirilmesine katkıda bulunmak.
- ✓ Okul sistemlerinin ve verilerin güvenliğinden sorumlu olmak.
- ✓ Bir dizi farklı çevrimiçi güvenlik konusundaki farkındalığa sahip olmak ve onların bakımında öğrencilerle nasıl ilişkili olabileceklerini bilmek.
- ✓ Yeni ve gelişmekte olan teknolojiler kullanıldığında iyi uygulamaları modellemek.
- ✓ Müfredat ile çevrimiçi güvenlik eğitimini ilişkilendirmek.
- ✓ Okul koruma politikalarını ve prosedürlerini takip ederek endişe duyan bireyleri belirlemek ve uygun önlem almak.
- ✓ Olumlu öğrenme fırsatlarına vurgu yapmak.
- ✓ Bu alanda mesleki gelişim için kişisel sorumluluk almak.

4.3. ÖĞRENCİLERİN BAŞLICA SORUMLULUKLARI ŞUNLARDIR:

- ✓ Okulun Kabul Edilebilir Kullanım Politikalarını okumak ve onlara bağlı kalmak.
- ✓ Çevrimiçi güvenlik politikalarının geliştirilmesine katkıda bulunmak.
- ✓ Çevrim içi ve çevrimdışı başkalarının hislerine ve haklarına saygı duymak.
- ✓ İşler ters giderse, güvenilir bir yetişkinden yardım istemek ve çevrimiçi güvenlik sorunlarıyla karşılaşan diğer kişileri desteklemek.
- ✓ Uzaktan çevrimiçi derslerde gerekmediği sürece kamerasını ve mikrofonunu kapalı tutmak. Canlı ders takibi sırasında kurallara uymak.
- ✓ Bireysel 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.

4.4. EBEVEYNLERİN BAŞLICA SORUMLULUKLARI ŞUNLARDIR:

- ✓ Okul Kabul Edilebilir Kullanım Politikalarını okumak, çocuklarını bu politikaya bağlı kalmaya teşvik etmek ve uygun olduğunca kendileri de bağlı kalmak.
- ✓ Çocuklarıyla çevrimiçi güvenlik konularını tartışmak, okulun çevrimiçi güvenlik yaklaşımlarını desteklemek ve evde uygun güvenli çevrimiçi davranışları pekiştirmek.
- ✓ Teknoloji ve sosyal medyanın güvenli ve uygun kullanımını modellemek.
- ✓ Davranışlarında, çocuğun çevrimiçi olarak zarar görme tehlikesi altında olduğunu gösteren değişiklikleri belirlemek.
- ✓ Okul veya diğer uygun kurumlardan, kendileri veya çocukları çevrimiçi problem veya sorunlarla karşılaşırsa yardım veya destek istemek.
- ✓ Okulun çevrimiçi güvenlik politikalarının oluşturulmasına katkıda bulunmak.
- ✓ Öğrenme platformları ve diğer ağ kaynakları gibi okul sistemlerini güvenli ve uygun bir şekilde kullanmak.
- ✓ Yeni ve gelişmekte olan teknolojilerin getirdiği fırsatlar ve risklerle ilgili olarak kendi bilinci ve öğrenimlerinden sorumlu olmak.

B. GİZLİLİK VE VERİLERİN KORUNMASI

1) İNTERNETİN KULLANILMASI VE OKUL CİHAZLARININ KÖTÜ AMAÇLI YAZILIMLARA KARŞI KORUNMASI

- Tüm okula ait cihazlar, okulun Kabul Edilebilir Kullanım Politikasına uygun olarak ve uygun güvenlik ve güvenlik önlemleri alınarak kullanılacaktır.
- Kötü amaçlı yazılım, meşru bir kullanıcının bilgisayarına virüs bulaştırmak ve birkaç yolla zararı artırmak için tasarlanan bir tür bilgisayar programıdır. Kötü amaçlı yazılım, bilgisayarlara ve cihazlara birkaç biçimde virüs bulaştırabilir ve çeşitli türleri vardır. Bunlara karşı dikkatli olmak ve koruyucu araçlar kullanmak çözüm olabilir. Kurumumuzda sınırlandırılmış bakanlık hattı kullanılmasının dışında yönetim bilgisayarlarında antivirüs programı yüklüdür.
- E-güvenlik politikamız Milli Eğitim Bakanlığı tarafından yayınlanan güvenli internet çerçevesine dâhildir. (Milli Eğitim Bakanlığı 2017/12 Sayılı Genelge)
- Okulumuz internet ağına, MEB SERTİFİKA güvenlik dosyası yüklenmeden internet ağına bağlanılamaz.
- İstenmeyen web sitelerini ve açılır pencereleri engellemek için, okuldaki cihazlarda kullanılan web tarayıcılarının güvenlik ayarları kişiselleştirilmektedir.
- 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.
- Çalışanların tüm üyeleri; çocukları korumak için tek başına filtrelemeye güvenmeyeceklerinin farkındadır ve gözetim-sınıf yönetimi-güvenli ve sorumlu kullanım eğitimi konusunda hassas davranmaktadır.
- 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.
- Tüm çalışanlarımız, velilerimiz, öğrencilerimiz etkili ve verimli çevrimiçi materyallerin kullanımı ve neden bu uygulamalara gerek olduğu konusunda düzenli eğitimlerle bilgilendirilmiştir.
- Personele dosya indirirken, taşınabilir cihazlar kullanırken, potansiyel virüslü dosyaları ve güvenli uygulamaları tespit edebilme için okul e-koordinatörü tarafından eğitim verilmektedir.
- E-güvenlik ve siber zorbalık konuları belli derslerimizin yıllık planlarına dahil edilmiş olup, bu konularda yıl içinde öğrencilere bilgi aktarımı devam etmektedir.

- İnternet kullanımı eğitimsel erişimin önemli bir özelliğidir ve tüm çocuklar bütünleşik okul müfredatının bir parçası olarak sorunlarını yanıtlamak için stratejiler geliştirmelerini destekleyecek ve onlara yardımcı olacak yaşa ve yeteneğe uygun eğitim alacaklardır. Bu eğitimler ders içi ve ders dışı olmak üzere ders müfredatları konu ve kazanımlarına göre ilişkilendirilerek verilecektir.
- E-koordinatör sene başı öğretmen kurul toplantısında duyurulur.
- Akıllı tahta kullanımı kontrollü/denetimli olmaktadır.
- Okul içerisinde proje için bile olsa sadece öğretmenlerin kayıtlı cihazları kullanılır.
- Diğer proje partnerleri ile iletişim ve görüntülü iletişim öğretmenler tarafından okul saatlerinde yapılmaktadır.

1.1. OKUL PERSONELİ GÜVENLİ İNTERNET KULLANIMI

- Personelimiz European Schoolnet (www.eun.org) tarafından yapılan eğitimlere katılmaktadırlar.
- Personelimizden bir kısmı eTwinning portalinden ve yerel/ulusal eğitimlerden e-güvenlik eğitimlerine katılmış ve sertifika almıştır. Bu personellerde bilgi paydaşlığı yapmaktadır. Almayan personelimiz de teşvik edilmektedir.
- Okulumuz personeli BIT koordinatörü tarafından eğitim almaktadırlar.
- Personel üyeleri, web sitelerini, araçlarını ve uygulamalarını sınıfta kullanmadan önce veya evde kullanmayı önerirken daima değerlendirecektir.
- Çevrimiçi güvenlik (e-Güvenlik) politikası, tüm çalışanların katılımı için resmi olarak sağlanacak ve tartışılacak ve korunma sorumluluğumuzun bir parçası olarak güçlendirilecek ve vurgulanacaktır.
- Personel, İnternet trafiğinin izlenebileceğini ve tek bir kullanıcıya kadar izlenebileceğinin farkında olacak. Okul sistemlerini ve cihazlarını kullanırken takdir yetkisi ve profesyonel davranış gereklidir.
- Personelin tüm üyelerine, profesyonel ve kişisel olarak, güvenli ve sorumlu İnternet kullanımı konusunda güncel ve uygun personel eğitimi, düzenli (en az yıllık) temelde çeşitli şekillerde sağlanacaktır.
- Çalışanların hepsi, çevrimiçi çevrimiçi davranışlarının okuldaki rolü ve itibarını etkileyebileceğinin farkına varacaktır.
- Mesleği veya kurumu tehlikeli durumuna düşürdüğü veya mesleki yeteneklerine güvenini kaybetmiş bir şeyin bulunduğu düşünülürse, hukuk, disiplin veya hukuki önlemler alınabilir.
- Filtreleme sistemlerini yönetme veya BİT kullanımını izleme sorumluluğu taşıyan personelin üyeleri, OGYE tarafından denetlenecek ve sorunları veya endişeleri bildirmek için açık prosedürlere sahip olacaklardır.

1.2. ÖĞRENCİLERİN GÜVENLİ İNTERNET KULLANIMI:

- Windows güvenlik duvarı uygulaması ve sınırlandırılmış MEB internet hattını kullanan öğrencilerimiz okul sınırları dâhilinde siber saldırılara maruz kalmamaktadır.
- Öğrencilere, okudukları veya gösterilen bilgilerin doğruluğunu kabul etmeden önce eleştirel düşünmeleri öğretilecektir.
- Öğrenciler, bilginin konumlanması, alınması ve değerlendirilmesi becerileri de dahil olmak üzere, internette araştırmada etkili kullanımı konusunda eğitilecektir.
- Belirli aralıklarla düzenli olarak; rehber öğretmenimiz ve bilişim öğretmenimiz öğrencilerimize "Siber zorbalık", "Akran zorbalığı", "Davranış geliştirme", "Güvenli ve Bilinçli İnternet Kullanımı", "Teknolojinin kullanımını kontrol" gibi konularda seminerler vermektedir.
- Adlarını ve aile bireylerinin adını aratarak internette ne tür bilgiler bulunduğuna bakmaları ve özel ya da uygunsuz olan her şeyi kaldırmaları istendi.
- Okulumuzda internetin kullanımı nasıl olacağı ile ilgili sabit/sürekli bir panomuz bulunmakta ve güncel halde tutulmaktadır.
- Her sene eTwinning proje paydaşlarıyla birlikte (2018'den beri) "Güvenli İnternet Günü"nü kutluyoruz.

1.3. İNTERNET KULLANIMI İÇİN EBEVEYNLERE TAVSİYELER

- Personel, çocukların internetin-dijital teknolojinin güvenilir ve sorumlu kullanıcıları olabilmesi için ebeveynlerin oynayacakları önemli bir role sahip olduklarını kabul eder.
- Okul Anlaşması'nın bir parçası olarak ebeveynlerin çevrimiçi güvenlik bilgilerini okumaları istenecektir. Ebeveynler, Okula Kabul Edilebilir Kullanım Politikası'nı okumaya ve çocuklarıyla etkilerini tartışmaya teşvik edilecektir.

- Çevrimiçi güvenlik konusundaki ebeveynler için bilgi ve rehberlik, ebeveynlere çeşitli biçimlerde sunulacaktır. Ebeveynler, çevrimiçi olarak çocukları için rol modeli olumlu davranışlar teşvik edilecektir.
- Evde güvenli internet kullanımı için gösteriler ve öneriler içeren ebeveyn eğitimleri sunulmakta olup; bu eğitim ve etkinliklere devam edilecektir.
- İnternetin güvenli kullanımı ile ilgili paketlerin tanıtım ve yaygınlaşmasını sağlamak devlet politikasıdır. Telekom buna yönelik güvenli internet paketi sunmaktadır. Evlerde limitli internet paketlerinin kullanımını teşvik etmek için rehberlik yapılmaktadır.
- Ebeveynleri denetim yolları ve teknolojik imkânları ile ilgili bilinçlendirmek ve gerekli uygulamaları geliştirmek ve yaygınlaştırmak için üniversiteden akademisyenlerden yardım alınmaktadır.
- Evde ve okulda ebeveynlerle çevrimiçi güvenlik konusundaki işbirlikçi, yaklaşımı teşvik edilecektir.
- Ebeveynlerin eğitimlere ve etkinliklerini katılımını sağlayabilmek için; çocuklarını da sürecin içine dahil ettiğimizi kanıtlayan bir yol izlenecektir. Okul panolarında ve web sitemizde bu faaliyetler afişlerle, duyurularla, sloganlarla desteklenmektedir.
- Aileye yönelik çocuk ve ergenlere denetimli, sınırlı ve amaçlı kullanım sağlayabilmeleri ile ilgili bilinçlendirme çalışmaları yapmaktayız.
- Öğrencilerin aktif olarak katılacağı sosyal projelerin arttırılacaktır.

İnternet kullanımı için; ebeveynlere kontrol sağlayacak, tavsiye ettiğimiz siteler ve uygulamalar:
WebWatcher, ScreenLimit, SecureTeen, MSPY, Qustodio uygulamalarını tavsiye ediyoruz.
https://www.internetyardim.org.tr/
http://www.gim.org.tr/ Daha Güvenli İnternet Merkezi.
https://www.guvenliweb.org.tr/ Güvenli Web - Çevrimiçi güvenlik konuları için farkındalık portali.
https://www.guvenlicocuk.org.tr/ Güvenli Çocuk - 13 yaşından küçük çocuklar için oyun/eğlence portali.
https://www.guvenlinet.org.tr/ Safer Internet Center'ın resmi sayfası.
https://www.ihbarweb.org.tr/ İhbar Web - Yasadışı içerik için telefon hattı.
https://www.guvenlioyna.org.tr/ Dijital Oyunlar Danışma Platformu
https://internet.btk.gov.tr/ İnternet BTK - İnternet ve BT yasası konusunda farkındalık portalı.
https://www.gig.org.tr/ SID Page - Daha Güvenli İnternet Günü Türkiye'de resmi sayfası.
sitelerini tavsiye ediyoruz.

2) OKULDAKİ HASSAS VERİLERİN KORUNMASI

- Personel ve öğrencilerin özlük işlemlerini yapan yöneticimizin kullandığı cihazda antivirüs programı kullanılmaktadır.
- Öğrencilere ve personele ait hassas veriler bilgisayarlarda veya dosyalarda saklanmamaktadır. Bu bilgiler Milli Eğitim Bakanlığına bağlı sitelerde yer almakta ve güvenlidir. Yönetici şifreleri belirli aralıklarla kişiler tarafından değiştirilmektedir. Ve bütün hareketler bakanlığın sitesinden izlenebilmektedir. Bütün personel şifrelerin nasıl olması gerektiği konusunda bilgilendirilmiş olup; doğum tarihi, yaşadığı şehir, sıralı rakam, aile bireyleri ismi gibi bilgiler olmayacak, en az 10 karakter, büyük küçük harf, sembol ve sayı kullanarak oluşturmaları belirtilmiştir. Her sene başında öğretmenlerin kullandıkları şifreleri güncellemeleri istenir. Herhangi bir şekilde şifresini unuttuğunu ve kurumsal olarak değişimini talep eden personelden yazılı dilekçe alınır ve talep ettiği kurallara uygun şifre verilir.
- Personele ait olan özlük dosyaları okul müdürü odasında kilitli dolaplarda saklanır. Okul müdürü ve sorumlu müdür yardımcısı dışında dosyaya kesinlikle erişim yasaktır.
- Öğrencilere ait özel bilgiler ya da kişisel bilgiler okulumuzda bulunmamaktadır. Bazı özel olmayan bilgiler şube rehber öğretmenler tarafından öğrenci tanıma formları doldurularak kendi dosyalarında saklanır. Önemli hassas bir durum görülürse okul rehber öğretmeni ve okul idaresine bildirilir.
- Önemli olan bilgilerin olduğu dosyalar için şifre konulur.
- Hassas verilerin korunması ile ilgili personele eğitim verilir ve sene başında bu konu ile ilgili protokol imzalatılır.
- Veri kayıplarını önlemek için düzenli yedeklemeler yapılmaktadır.
- Velilerimizin ve personelimizin iletişim bilgileri kendi bilgi ve istekleri haricinde asla 3. şahıslarla paylaşılamaz.

❖ Personel ve öğrenci girişi dışında giriş çıkışlar kontrollü sağlanmakta olup; ziyaretçi defteri tutulmaktadır. Veliler randevu alarak görüşme talep ederler.

3) OKULDAKİ MOBİL CİHAZLARIN KULLANILMASI

3.1. KİŞİSEL CİHAZ VE CEP TELEFONLARININ KULLANIMI:

- Cep telefonlarının ve diğer kişisel cihazların yaygın bir şekilde sahiplenilmesi, tüm üyelerin cep telefonlarının ve kişisel cihazların sorumlu bir şekilde kullanılmasını sağlamak için gerekli adımları atmalarını gerektirir.
- Namık Kemal Ortaokulu, mobil teknolojilerle yapılan kişisel iletişimin, çocuklar, personel ve anne-babalar için gündelik yaşamın kabul edilen bir parçası olduğunun farkındadır; ancak, bu tür teknolojilerin okulda güvenli ve uygun bir şekilde kullanılmasını gerektirir.
- Çocukların ve yetişkinlerin cep telefonlarının ve diğer kişisel cihazların kullanımı, okul tarafından kararlaştırılacak ve Cep Telefonu Politikasında yer alacaktır.
- Öğretmenlerle (eğitim öğretim başında, ortasında ve sonunda olmak üzere) yılda üç kez yapılan öğretmenler genel kurulunda okul güvenliği ve dolayısıyla cep telefonu politikası hakkında değerlendirme amaçlı tartışmalar yapılır. Ve karar alınarak kurul defterine işlenir.
- Velilerle her yıl, eğitim öğretim yılı başında cep telefonu kullanımı konusunda kurul kararı hakkında ve kararların neden alındığı konusunda bilgi verme amaçlı toplantılar yapılır. Toplantı sonunda velilere bütün yasal sorumluluğun öğrenci ve veliye ait olduğu bir sözleşme imzalatılır. (Bütün ılımlı politikaya ve konuşmalara rağmen imzalamak istemeyen veli olursa; eGüvenlik komisyonu tarafından durum tutanak altına alınır.)

3.2. ÖĞRENCİLERİN KİŞİSEL CİHAZLARINI VE CEP TELEFONLARINI KULLANIMI:

- Öğrenciler, kişisel cihazların ve cep telefonlarının güvenli ve uygun kullanımı konusunda eğitim alacaklardır.
- Bilişim araçlarını, okul yönetimi ile öğretmenin bilgisi ve izni dışında konuşma yaparak, ses ve görüntü alarak, mesaj ve e-mail göndererek, bunları arkadaşlarıyla paylaşarak eğitim-öğretimi olumsuz yönde etkileyecek şekilde kullanmak aynı zamanda okul ders saatleri içerisinde telefon bulundurmak kesinlikle yasaktır.
- Herhangi bir sebeple cep telefonlarını okula getirmek zorunda kalan öğrenciler, telefonlarını okula girişinden itibaren kapalı konumda tutmakta, okul yönetici odasında telefonlar için yapılmış olan özel bölüme koymaktadır.
- Okulda öğrencilerin telefon kullanımın yasak olduğu afişleri okul duvarında asılıdır.
- Cep telefonunun amacı dışında kullanımı ihlali oluştuğunda, öğrenci, telefondaki özel verilerin korunmasını sağlamak amacıyla telefonunu kapatıp ders öğretmenine verir. Ders öğretmeni öğrenci telefonunu ilgili müdür yardımcısına teslim eder. Durum tutanakla kayıt altına alınır. Cep telefonu öğrenci velisine teslim edilinceye kadar güvenli bir yerde tutulur. Velisi dışında telefon kimseye teslim edilmez.
- Cep telefonunu yönetime teslim etmeyen ve cep telefonu ile okul içerisinde video ya da fotoğraf çeken öğrencilere yasaların ve Ortaöğretim Kurumları Yönetmeliğinin Ödül ve Disiplin maddeleri gereği işlem yapılmaktadır.
- Öğrencinin kişisel cihazında veya cep telefonunda bulunan materyalin yasadışı olabileceği veya cezai bir suçla ilgili kanıt sağlayabileceğinden şüpheleniliyorsa, cihaz daha ayrıntılı araştırma için polise teslim edilir.
- 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.
- Çocukların cep telefonlarının ve kişisel cihazların tüm kullanımları, kabul edilebilir kullanım politikasına uygun olarak gerçekleşecektir. Cep telefonları veya kişisel cihazlar, bir öğretmenin onayını alarak onaylanmış ve yönlendirilmiş müfredat tabanlı etkinlik kapsamında olmadıkları sürece dersler veya resmi okul saatlerinde öğrenciler tarafından kullanılamaz.
- Çocukların cep telefonlarını veya kişisel cihazlarını eğitim etkinliğinde kullanımı, okul idaresi tarafından onaylandığında gerçekleşecektir.

- Bir öğrenci ebeveynlerini arama gereği duyduğunda, okul telefonunu kullanmasına izin verilecektir.
- Velilerimiz okul saatleri içerisinde öğrencileriyle görüşme yapmamaları 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.
- Öğrencilere, cep telefonlarının ve kişisel cihazların güvenli ve uygun bir şekilde kullanımı öğretilecek ve sınırların ve sonuçların farkına varılacaktır.
- Okul sınırları içerisinde herhangi bir öğrencinin wi-fi bağlantısına erişmesine izin verilmez. Diğer ifadeyle öğrencinin herhangi bir yolla şifreyi elde edip kablosuz ağ bağlantısına bağlanması yasaktır. Bu yasağı ihlal ettiği tespit edilen öğrencinin cep telefonuna el konulur. Gerekli işlemler yapılır. (Ders görevi olması ve araştırma yapması gerektiği durumlarda okul idaresi tarafından kullanıma süreli izin verilmektedir.)

3.3. PERSONEL (YÖNETİCİ/ÖĞRETMEN/ÇALIŞAN) KİŞİSEL CİHAZLARINI VE CEP TELEFONLARINI KULLANIMI:

- Çalışanlar (öğretmen, idareci, personel vb) okul politikasına aykırı davranışlarda bulunursa disiplin işlemleri başlatılır.
- Çalışanlar (Yönetici, dersi olmayan öğretmen, personel vb) kişisel cep telefonlarını ders saatlerinde sessize alarak ya da kapatarak görevlerine devam etmelidir.
- Okulumuzda bulunan öğretmenlerimiz derslere girerken telefonlarını kapatarak ya da sesini kısarak; şahsi kilitli dolaplarına koymakla yükümlüdür. Etkileşimli ders işleyecek olan öğretmen varsa ve telefon kullanması gerekiyorsa ders öncesi yöneticilere bilgi vermekle yükümlüdür. Bu durum öğretmenler kurul kararlarında belirtilmiş, afişlerle okul duvarında yerini almıştır.
- 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.

3.4. ZİYARETÇİ KİŞİSEL CİHAZLAR VE CEP TELEFONLARININ KULLANIMI:

- Ebeveynler ve ziyaretçiler, okulun kabul edilebilir kullanım politikasına uygun olarak cep telefonlarını ve kişisel cihazları kullanmalıdır.
- Fotoğraflar veya videolar çekmek için ziyaretçiler-ebeveynler tarafından cep telefonlarının veya kişisel cihazların kullanılması, okul resim kullanımı politikasına uygun olarak gerçekleştirilmelidir.
- Okul, ziyaretçilere kullanım beklentilerini bildirmek için uygun tabelaları/bilgileri sağlayacak ve sunacaktır.
- Personelin uygun ve güvenli olduğunda sorunlara karşı çıkması beklenir ve her zaman ziyaretçilerin herhangi bir ihlalini idareye bildirecektir.

3.5. OKULUMUZDA FOTOĞRAF YA DA VİDEO ÇEKİMİ

- Okul idaresi tarafından görevli kılınanlar haricindeki kişiler tarafından ve öğrenci velilerinin bilmek istedikleri etkinlik/programlar dışındaki zamanlarda, okul ve okul bahçesi sınırları içerisinde fotoğraf ve video çekimi yapılamaz. Bu yasak bir öğrencinin diğer bir öğrencinin fotoğraf ve videosunu çekmek istemesi durumunda da geçerlidir. Kullanımın yasak olduğu afişleri okul duvarında asılıdır ve web sitemizde yer almaktadır.
- Okul idaresi tarafından görevlendirilen kişilerin çektiği fotoğraf ve videolar ancak okulun resmi web adresinde, ilgili öğrenci velisinin talep ve yazılı onayı ile yayınlanabilir. Öğrencisi için onay vermeyen velinin öğrencisi ile ilgili fotoğraf ve videolar yayınlanmaz. Velisi tarafından fotoğraf ve video görüntülerinin çekilip yayınlanmasına onay verilmeyen öğrencilerin, çekim esnasında psikolojik baskı yaşamaması için tedbirler alınır.
- Okul görevlileri tarafından yayınlanan resim ve videolarda öğrencilerin kişisel bilgilerine kesinlikle yer verilmez ve zorunlu haller dışında yüzü görünmez.
- Öğrenciler, bir video konferans araması veya mesajı hazırlamadan veya cevaplamadan önce

sorumlu bir öğretmenden izin isteyecektir. Video konferans, öğrencilerin yaşı ve yeteneği için uygun bir şekilde denetlenecek. (Okul bunun nasıl uygulanacağını ve başarılacağını listeler.)

3.6. ÇEVRİMİÇİ GÖRÜNTÜ VE VİDEOLAR YAYINLAMA

- Okul, çevrimiçi paylaşılan tüm resimlerin ve videoların okul resim kullanımı politikasına uygun şekilde kullanılmasını sağlayacaktır.
- Okul, resimlerin ve videoların tümünün, veri güvenliği, Kabul Edilebilir Kullanım Politikaları, Davranış Kuralları, sosyal medya, kişisel cihazların ve cep telefonlarının kullanımı gibi diğer politikalar ve prosedürlere uygun şekilde yer almasını sağlayacaktır.
- Görüntü politikasına uygun olarak, öğrencilerin resimlerinin/videolarının elektronik olarak yayınlanmasından önce her zaman ebeveynlerin yazılı izni alınacaktır.
- Veli izni yanında öğrencinin de izni alınacaktır.
- Öğrenciler tarafından hazırlanacak olan bir video henüz hazırlanmadan önce, bununla ilgili görev alan öğrenciler, öğretmenlerinden izin almalıdır.
- Kullanıcılar, şahsi sosyal medya hesaplarında, okul öğrencileri ve çalışanlarının yer aldığı görselleri paylaşamazlar.
- Video konferans, sağlam bir risk değerlendirmesini takiben, resmi ve onaylanmış iletişim kanalları vasıtasıyla gerçekleşecektir.
- Video konferans yapılırken, tüm kullanıcıların katılabileceği siteler üzerinden yapılacaktır.
- Video konferans yapılmadan önce diğer okullarla iletişim kurulmuş olması gerekmektedir.
- Sadece ana yöneticilere video konferans yönetim alanlarına veya uzaktan kumanda sayfalarına erişim hakkı verilmektedir.
- Eğitimli video konferans servisleri için benzersiz oturum açma ve şifre bilgileri yalnızca personel üyelerine verilecek ve güvence altına alınmış olacak.
- Okul öğrenci ve çalışanlarını ilgilendiren/içinde bulunduran tüm içerik, ancak kontrol ve onay süreçlerinden geçtikten sonra, paylaşıma açık hale gelecektir.
- Velilerin rızası, öğrenciler video konferans faaliyetlerine katılmadan önce edinilecektir.

4) ŞİFRE DEĞİŞİKLİKLERİ

- 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 makul önlemleri almalıdır. Şifrelerini başka bir kişiyle paylaşmamalı ve şifrelerini düzenli olarak değiştirmelidir. Bir kullanıcı hesabına ait şifre kullanılarak gerçekleştirilen her türlü işlemden, söz konusu işlemi gerçekleştiren taraf hesap sahibinin kendisi olmasa dahi sorumlu hesap sahibidir.
- Bilişim Teknolojileri öğretmenimiz bu konuyla ilgili sitemiz üzerinden bilgilendirme yapmış olup, okulda da çeşitli seminerler/eğitimler düzenlemiştir.

Eğitimlerde;

-Bilgisayardan ve cep telefonlardan uzaklaşıldığında her zaman bilgisayar programlarındaki oturumun kapatılması ve parolalı bir ekran koruyucu kullanılması tavsiye edildi.

-İyi parola yönetimi ve güvenliği konusunda alıştırma yapılması, parolalarını hiçbir zaman başkalarıyla paylaşmamaları ve parolalarınızı sık sık değiştirmeyi unutmamaları belirtildi.

***Bütün personel ve öğrenciler; şifrelerin nasıl olması gerektiği konusunda bilgilendirilmiş olup; doğum tarihi, yaşadığı şehir, sıralı rakam, aile bireyleri ismi gibi bilgiler olmayacak, en az 10 karakter, büyük küçük harf, sembol ve sayı kullanarak oluşturmaları belirtilmiştir. Her sene başında öğretmenlerin kullandıkları şifreleri güncellemeleri istenir.

C. TELİF HAKLARI KULLANIMI

*** 1948 Tarihli Birleşmiş Milletler Genel Kurulu'nda kabul edilen İnsan Hakları Evrensel Bildirgesi'nin

27'inci Maddesi:
"1. Herkes toplumun kültürel faaliyetine serbestçe katılmak, güzel sanatları tatmak, bilim alanındaki ilerleyişe katılmak ve bundan yararlanmak hakkına sahiptir.
2. Herkesin sahibi bulunduğu (yarattığı) her türlü bilim, edebiyat veya sanat eserinden doğan manevi ve maddi yararlarını korunmasını isteme hakkı vardır." Şeklindedir.

*** https://www.telifhaklari.gov.tr/ (T.C. KÜLTÜR VE TURİZM BAKANLIĞITELİF HAKLARI GENEL MÜDÜRLÜĞÜ) adresinden bilgi alınabilmektedir.
*** Telif Hakkının doğması için tescile gerek yoktur. Fikir ve sanat eserleri üzerindeki haklar eserin üretilmesiyle birlikte doğar.
***Telif hakları soyut niteliğe sahiptir. Telif hakları ile koruma altına alınan, insan düşüncesinin yarattığı maddi olmayan mallardır. Telif hakları somutlaştığı maddeden ayrı ve bağımsız bir varlık ve hukuki değere sahiptir.
***Telif haklarında ülkesellik ilkesi geçerlidir. Koruma hangi ülkede talep ediliyorsa koruma şartları o ülke mevzuatına göre belirlenir.

Eser sahipleri eserlerinin elektronik ortama aktarılma işlemlerini telifine uygun olarak kendileri yerine getirebilirler. Günümüzde açık erişim hareketini destekleyen yayınevlerinin sayısı her geçen gün atış göstermektedir.Dergi yayıncılarının telif hakları ve kişisel arşivleme politikaları SHERPA/ROMEO listesinden kontrol edilebilir ve depolama yapılabilir. Ayrıca resimler için FLICK, albümler için JOMENDO, medya için SPINXPRESS tavsiye edilmektedir.
Yazarların yayınlarının kullanım haklarını kendilerinin belirlediği Creative Commons lisanslarının kullanımı teşvik edilmektedir.

D. SOSYAL AĞLAR VE SOYAL MEDYA

1) OKUL/WEB SİTESİNİN YÖNETİLMESİ

⇒ Okulumuzun Milli Eğitim Bakanlığı tarafından atanmış bir resmi web sitesi bulunmaktadır.
⇒ Web sitesinde iletişim bilgileri okul adresi, e-posta ve telefon numarası olacaktır. Personel veya öğrencilerin kişisel bilgileri yayınlanmayacaktır.
⇒ Okul Müdürü yayınlanan çevrimiçi içerik için genel yayın sorumluluğunu alacak ve bilgilerin doğru ve uygun olmasını sağlayacaktır.
⇒ Web sitesi, erişilebilirlik fikri mülkiyet haklarına saygı, gizlilik politikaları ve telif hakkı da dahil olmak üzere okulun yayın yönergelerine uyacaktır.
⇒ Spam maillerden korunmak için e-posta adresleri çevrimiçi olarak dikkatli bir şekilde yayınlanacaktır.
⇒ Öğrenci çalışmaları öğrencilerin izniyle yayınlanacaktır.
⇒ Okul web sitesinin yönetici hesabı, uygun bir şekilde güçlü şifreyle şifrelenerek korunacaktır.
⇒ Okul, çevrimiçi güvenlik dahil olmak üzere, toplumun üyeleri için okul web sitesinde korunma hakkında bilgi gönderecektir.
⇒ Web sitemizde öğrencilerin etkinlikleri, eTwinning projeleri çalışmaları, çeşitli seminerlerin duyuruları, genel müdürlük ve bakanlığımızın çalışmaları ve duyuruları, belirli gün ve hafta etkinlikleri, yapılan projelerin çalışmalarını paylaşıyoruz. Mümkün olduğu kadar kişilerden ziyade etkinlikleri paylaşıyoruz.

Yaptığımız paylaşımlarda yer alan şahıslardan kişisel yazılı izin belgeleri(personelin kendisinden, öğrencinin kendisi ve velisinden) alınmış olup; kişisel verilerin korunması ve özel hayatın gizliliği ilkelerine dikkat ediyoruz.

2) SOSYAL MEDYA KULLANIMI

⇒ Okulumuzun sosyal ağ olarak sadece Facebook hesabı bulunmaktadır. Bu ağların üzerinde yayınlanan veriler kontrollü olarak paylaşılmaktadır. Bu ağlarda okulumuz bir engelli okulu olduğu için; farkındalık yaratma, sosyal algı ve empati geliştirme, etik değerleri yansıtma, bireysel farklılıklara saygı duyma içerikli paylaşımlar yapıyoruz.
⇒ Yaptığımız paylaşımlarda yer alan şahıslardan kişisel izin belgeleri alınmış olup; kişisel verilerin korunması ve özel hayatın gizliliği ilkelerine dikkat ediyoruz. Her ne kadar yazılı izin belgeleri alınmış olsa da yüzlerinin görünmemesine özen gösteriyoruz.

2.1. ÖĞRENCİLERİN SOSYAL MEDYA HESAPLARI
⇒ Öğrencilerimiz görme engelli ve yaşı küçük olduğu için sosyal medya hesapları aileleri tarafından açılmasına izin verilmemektedir.
⇒ Öğrencilerimiz facebook, instragram, twitter gibi hesapları açmak istemeleri durumunda ne şekilde davranmaları ve nelerden sakınmaları gerektiği, bulundukları sosyal ağın davranış kurallarına ve etik değerlere dikkat etmeleri gerektiği, çeşitli cinsel içerikli ya da yasadışı paylaşımlara maruz kalabilecekleri özel mesajlara karşı geliştirmeleri gereken tutumların nasıl olması gerektiği konusunda okulumuz eGüvenlik koordinatörü tarafından bilgilendirme seminerlerine alınmıştır.

E. ETWINNING DIŞINDAKİ ÇEVRİMİÇİ İLETİŞİMİN ZORLUKLARI

1) ZORLUKLAR VE DAVRANIŞ GELİŞTİRME -TEDBİRLER
- Okulumuzun tüm üyeleri çevirimiçi riskler konusunda bilgilendirilecektir. Eğitimler yapılıp içerikler açıklanacaktır.
- Okulumuzda yasadışı içerik, güvenlik ihlali, siber zorbalık, cinsel içerikli mesajlaşma, çocuk istismarı, kişisel bilgi güvenliği gibi konularda bilgilendirme çalışmaları yapılmaktadır.
- Okulumuzda internet, bilgi teknolojileri ve ekipmanlarının yanlış kullanımı ile ilgili tüm şikâyetler okul müdürüne bildirilecektir. Müdürlük tarafından gerekli denetimler ve düzenlemeler yapılacaktır.
- 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.
- Bir öğrenci herhangi bir mağduriyet yaşar ve personelden herhangi biriyle paylaşırsa, ne şekilde hareket edilmesi gerektiği konusunda (yasal, psikolojik, teknik) personel bilgilendirilecektir.
- https://www.connectsafely.org/tips-to-help-/stop-cyberbullying
  https://cyberbullying.org/resources/parents sitelerini takip ve tavsiye ediyoruz.

2) SİBER ZORBALIK

Siber saldırı çok çeşitli yöntemlerle gerçekleştirilebilir. Solucanlar, trojenler, virüs indirmesine olanak tanıyan sahte mailler ve çeşitli yöntemlerle her gün yüz binlerce siber saldırı gerçekleştirilmektedir. Siber saldırıların sonuçları tahmin ettiğimizden de büyük olabilir.

Siber saldırı iki şekilde olur. İlkinde kişilerin şifreleri ele geçirilir, web sitelerine yönelik saldırılar düzenlenir, virüs taşıyan mesajlar ve spam mesajlar yollanarak elektronik saldırı uygulanır.
İkincisi daha tehlikeli bir saldırıdır. Burada tamamen kişiyi aşağılamak, küçük düşürmek, onu zor durumda bırakmak için psikolojik bir saldırı uygulanır.

Siber saldırılardan korunmak için yapılan çalışmalar ve öneriler şunlardır:
- Bütün öğrencilere ve personele, Siber Tuzaklar Kamu Spotu izletildi.
http://www.eba.gov.tr/video/izle/47943f13fb2849bb04ecf885e6d67d600f1498e0b4001
- Ayrıca http://www.guvenlicocuk.org.tr/ , https://www.gig.org.tr/ , adreslerinden internet güvenliği ile ilgili video, afiş vb. çalışmalardan öğrencilerimizin seviyelerine uygun olanlar kullanılmıştır.
- Emniyet Müdürlüğü yetkililerince okulumuz öğretmen-öğrenci ve velilerine yönelik Güvenli İnternet bilgilendirmesi yapılması için davet edilmiştir.
- Bilişim Teknolojileri öğretmenimiz bu konuyla ilgili sitemiz üzerinden bilgilendirme yapmış olup, okulda da çeşitli seminerler düzenlemiştir.

Eğitimlerde;

*Bilgisayardan ve cep telefonlardan uzaklaşıldığında her zaman bilgisayar programlarındaki oturumun kapatılması ve parolalı bir ekran koruyucu kullanılması tavsiye edildi.
*İyi parola yönetimi ve güvenliği konusunda alıştırma yapılması, parolalarını hiçbir zaman başkalarıyla paylaşmamaları ve parolalarınızı sık sık değiştirmeyi unutmamaları belirtildi.
*Adlarını ve aile bireylerinin adını aratarak internette ne tür bilgiler bulunduğuna bakmaları ve özel ya da uygunsuz olan her şeyi kaldırmaları istendi.
*Güvendikleri kişilerin dışındakiler ile çevrimiçi paylaşımlarını sınırlamak için tüm çevrimiçi hesaplarında gizlilik ayarlarını kullanmaları söylendi.
*Birisinin bir kimlik avı saldırısı veya virüs bulaşmış olan bir web sitesi aracılığıyla bilgisayarlarına casus yazılım yüklemesini önlemek için iyi, güncellenmiş güvenlik yazılımı kullanmaları tavsiye edildi.
*İçinden çıkılamayacak bir duruma gelmeden bir yetişkinden ya da bir uzmandan yardım istemeleri belirtildi.
*Herhangi bir şekilde olumsuz bir fotoğraf, tehdit, mesaj vs. aldıkları zaman kesinlikle kanıtları saklamaları, herhangi bir şekilde cevap vermemeleri gerektiği belirtildi.
➢ Personele ve velilerimize; öğrencilere yasaklamalar yapmak yerine, nedenleri ve süreçte yaşanabilecek sorunları, herhangi bir sorunla karşılaşma durumunda nasıl hareket edilmesi gerektiğini anlatıyoruz. https://www.childnet.com/ sitesini takip etmelerini tavsiye ediyoruz.

F. GÜVENLİ İNTERNET GÜNÜ

1) GÜVENLİ İNTERNET GÜNÜ

Öğrencilere, öğretmenler ve ebeveynlere "Güvenli İnternet Kullanımı" ile ilgili bilgilendirme seminerleri yapılmaktadır. Bununla ilgili bir ekip kurulmuştur. Ekip başkanı olarak kurum müdür başyardımcısı Deniz YAPICI, üyeler olarak da Bilişim Teknolojileri Öğretmeni Engin ÜLGER, Rehber Öğretmen Dinçer ÖZTÜRK, Özel Eğitim Öğretmeni Osman ARSLAN, Din ve Etik Öğretmeni Murat ÇOPUR belirlenmiştir. Bunun dışında okulumuz web sitesinde bunlarla ilgili haberler yayınlanmaktadır.

Okulumuzda Güvenli ve Bilinçli İnternet Kullanımı, eTwinning, e-Güvenlik, Siber Zorbalık ile ilgili sabit panolar bulunmaktadır. Ayrıca okulumuzda herkesin göreceği açık bir alanda bunlarla ilgili uyarıların ve yaygınlaştırma çalışmalarının bulunduğu ayrı bir alan vardır.

6 Şubat İnternet Günü 2018 yılından beri okulumuzda kutlanmaktadır.

- Her sene düzenli olarak yürütülen eTwinning projelerinde internet günü kutlaması etkinliklerine yer verilmektedir.
- Hafta boyunca seminerler, tanıtıcı afişler ve webinarlar düzenlenmekte, etkin katılım sağlanmaktadır.
- Okulumuz öğretmenleri e twinning portalında, safer ınternet SİD 2018, facebook hesaplarında paylaşım yapmışlardır.
- Veli ve öğrencilere eğitici ebeveyn ve öğrenci bilgilendirici videoları sunuları izletilmiştir. Okumuzda çeşiti web2 araçları kullanılarak sunular hazırlanmış, panolar ailelerle birlikte hazırlanmıştır
- http://guvenlinet.org.tr/tr/ sayfasından bilgi amaçlı faydalanılmıştır

2) e- GÜVENLİK EĞİTİMLERİ

2.1.e-GÜVENLİK EĞİTİMİNİN GENEL İLKELERİ:

- e-Güvenlik çok çeşitli konuları kapsar ve tek başına görülmemektedir.
- Tüm personelin e-Güvenlik konusunda eğitim alması sağlanmaktadır.
- Personel, öğrencilerin alışkanlıklarındaki ve kullandıkları teknoloji ve uygulamalardaki değişiklikleri dikkate almak için yılda en az bir kez güncellenmektedir.
- Hizmet içi eğitimi doğru bir şekilde hedeflemek için okuldaki personelin eğitim ihtiyaçları denetlenmektedir.
- Bir okul, e-Güvenlik'in koordinasyonundan sorumlu belirlenmiş bir kişiye sahip olmanın yararlı olup olmayacağını düşünmek isteyebilir, ancak e-Güvenlik'in her personel üyesinin sorumluluğunda olduğu açıkça belirtilmektedir.

2.2. e-GÜVENLİK İLE İLGİLİ EĞİTİMLER/SEMİNERLER

Okulumuzda bir eGüvenlik Komisyonu oluşturulmuş olup; görev dağılımı ile öğretmenler, öğrencilere, velilere eğitimler/seminerler verilmektedir. Bu paylaşım şu şekildedir:

***Proje ekibi başkanı tarafından eTwinning portali ve projeleri, eSafety konusundaki duyarlılıklar ve okul politikası, eSaferday, Erasmus+ Projeleri, Scientix, SchoolEducationGatawey vs …
***Rehberlik öğretmeni tarafından, 5-6-7 ve 8. sınıflara düzenli olarak, Mahremiyet, Akran zorbalığı, Psikososyal müdahale koruma ve krizi önleme, Davranış geliştirme...
***Bilişim Teknolojileri öğretmeni tarafından BİT bağımlılığı, BİT‟nin doğru ve güvenli kullanımı, Siber zorbalık, Web güvenliği, Dijital vatandaşlık…
***Din Kültürü ve Ahlak Bilgisi öğretmeni tarafından Etik, Mahremiyet, Ahlaklı davranış geliştirme…
***Türkçe öğretmeni tarafından iletişim, kendini ifade etme...
gibi konularda seminerler/eğitimler/toplantılar tertiplenmektedir. Bu toplantılar için duyuru afişleri hazırlanarak web sitemizde ve okul panomuzda ayrıca sergilenmektedir. Öğretmenlerimize ve diğer personelimize resmi yazılarla tebliğ edilmektedir.
***Bilgisayar Teknolojileri dersinde internet etiği ve güvenli internet kullanımı konuları öğrencilerimize aktarılmaktadır.

- EBA eğitim ve eTwinning portalleri kullanımı yoğun olup; zümre öğretmenleri tarafından her zümrede BİT‟nin doğru ve güvenli kullanımı, yapılan alıntıların derslere ve ödevlere aktarımı(kaynak kullanımı) ile ilgili kararlar alınmakta ve öğrenciler bu yönde bilgilendirilmektedir.
- Okulumuzun personeli Milli Eğitim Bakanlığı tarafından verilen “Siber Zorbalık, BİT’in doğru ve güvenli kullanımı, Web 2.0 araçları, Robotik ve Kodlama, Dijital Araçların Kullanımı, Web 2.0 . Araçları” konularında uzaktan ve yüz yüze eğitimler almıştır/alacaktır.
- Ayrıca eTwinning üyesi olan öğretmenlerimiz http://etwinningonline.eba.gov.tr/ adresinden İngilizce ve Türkçe olan eğitimleri takip etmektedir. Ve katılan personellerimiz sertifika sahibidir. Yine portale üye olan öğretmenlerimiz www.etwinning.net adresinden mesleki çalışmalara aktif olarak katılmaktadır.
- Tüm öğretmenlere, ebeveynlere ve öğrencilere gizlilik ve güvenlik, dijital ayak izi ve itibar, siber zorbalık, bilgi okuryazarlığı, davranış geliştirme, akran zorbalığı, etik ve benzeri konularda düzenli eğitim/seminer verilmektedir.

2.3. E-GÜVENLİK KONULARININ MÜFREDATIMIZA AKTARILMASI

e-Güvenlik'in müfredatın bir parçası olarak öğretilmesini benimsiyoruz.

BİT veya medya ile ilgili kurslarda e-Güvenliği anlatırken, e-Güvenlik ve diğer müfredat alanları arasındaki birçok bağlantıyı araştıran daha kapsamlı bir müfredatlar arası yaklaşım izliyoruz.

• Medya okur-yazarlığı ve bilişim derslerinde internet kullanımı ile ilgili içerik güncel ve teknolojik gelişmeler ışığında güncellenmiştir. Çocuklarda bilinçli ve güvenli internet kullanımına dair bilgi, beceri ve tutumların geliştirilmesi için seminerler düzenlenmektedir.

• Türkçe, Sağlık Bilgisi, Fen Bilimleri vb ilgili derslerde uygun şekilde işlenmesi sağlanmaktadır.

•Ders müfredatlarına sosyal medya başta olmak üzere internetin bilinçli kullanımı ile ilgili konuların yenilenen bilgilerle güncellenmesi okul BİT koordinatör öğretmeni tarafından sağlanmıştır.

•Fatih projesinin yürütülmesi ve sürdürülmesi aşamasında teknolojinin etkili ve güvenli kullanımlarının sağlanması için BTK tarafından güvenli internet ağı mevcuttur.

• MEB’e bağlı okullarda elektromanyetik kirliliğe ve internet güvenliğine önem verilmektedir.

G. FARKLI MESLEK GRUPLARININ KATKISI

-eGüvenlik konularındaki eğitimlerde karşılıklı protokol imzaladığımız Emniyet Müdürlüğünden personel davet ederek; eğitim talep ediyoruz.

-Okul formatörü ayda bir kere okul cihazlarını kontrol ediyor.

H. YÖNTEM

Kabul Edilebilir Kullanım Politikası

Namık Kemal Ortaokulu bilgisayar sistemlerini birçok kullanıcı paylaşmaktadır. Bu sistemler dikkatli bir şekilde kullanılmalıdır; bir kaç 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:

- Okul, Okula ait bilgisayar sistemleri üzerindeki tüm hak, mülkiyet ve çıkarlara sahiptir. Namık Kemal Ortaokulu Kabul Edilebilir Kullanım Politikası veya bilgisayar sistemlerin kullanımına ilişkin olarak okul tarafından herhangi bir mecrada yayımlanan hüküm ve koşullar altındaki hiçbir hüküm hiçbir şekilde söz konusu hak, mülkiyet ve çıkarların kullanıcılara devredildiği anlamına gelmemektedir. Okul kullanıcılara sadece bilgisayar sistemlerinin kullanımına ilişkin şahsi, dünya genelinde, bedelsiz, devredilemeyen ve münhasır olmayan bir lisans tanımaktadır. Kullanıcılar bilgisayar sistemlerinin hiçbir yazılım veya diğer bir parçasını kopyalayamaz, değiştiremez, yeniden üretemez, bunlardan türemiş çalışma yaratamaz, tersine mühendislik yapamaz, parçalara ayıramaz veya diğer bir şekilde kaynak koduna dönüştüremez.
- Kullanıcılar, okulun izin vermediği bilgisayar sistemlerini kullanamazlar. Bilgisayar sistemlerine erişebilmek için hatalı veya aldatıcı bilgilerin temin edilmesi suretiyle vs şekillerde bilgisayar sistemlerinin yetkisiz kullanımı yasaktır. Kullanıcılar diğer kurum, kuruluş veya kişilerin bilgisayar sistemlerine yetkisiz erişim sağlamak için okulun bilgisayar sistemlerini kullanamaz.
- 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 makul önlemleri almalıdır. Şifrelerini başka bir kişiyle paylaşmamalı ve şifrelerini düzenli olarak değiştirmelidir. Bir kullanıcı hesabına ait şifre kullanılarak gerçekleştirilen her türlü işlemden, söz konusu işlemi gerçekleştiren taraf hesap sahibinin kendisi olmasa dahi sorumlu hesap sahibidir.
- Okulun bilgisayar sistemleri yalnızca izin verildiği şekilde okul ile ilişkili hususlarda 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 yayımlanan 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, 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.
- Okula ait hiçbir bilgisayar sistemi sorumsuz bir şekilde veya başkalarının işlerine engel olacak şekilde kullanılamaz. Buna; hakaret içerikli, rahatsız edici veya taciz edici içerikler ile zincirleme mektup, yetkisiz toplu mail veya istenmeyen reklamların iletilmesi veya ulaşılabilir kılınması; kullanıcıya ait olmayan bir sistem, materyal veya bilgiye kasıtlı, dikkatsizce veya ihmalkâr bir biçimde zarar verilmesi; kasıtlı olarak elektronik iletişimin kesintiye uğratılması veya diğer bir şekilde başkalarının mahremiyetinin ihlal edilmesi veya kullanıcıya ait olmayan veya kullanıcı için olmayan bilgiye erişilmesi; sistem kaynaklarının kasıtlı olarak hatalı kullanılması veya başkalarının hatalı kullanmasının sağlanması veya ücretsiz yazılım gibi güvenilir olmayan kaynaklardan idari sistemlere yazılım veya veri indirilmesi dâhildir.
- 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 GİBİ" ve "MEVCUT HALİYLE" 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 yükleme yapacak içeriklerin yüklenmesinin; (iii) bilgisayar sistemlerinin genel güvenliğine tehlike arz edecek ve/veya diğer kullanıcıları zarara uğratacak 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 "by-pass" edilmesine ilişkin her türlü bilginin tespiti durumunda, vakanın Namık Kemal Ortaokulu Bilgi Teknolojileri Direktörlüğü'ne ya da E-Güvenlik Koordinatörlüğü'ne bildirilmesi zorunludur.

❖ Okul bilgisayar sistemlerinin yetkisiz veya uygunsuz bir şekilde kullanımı, işbu politikaya uyulmaması dâhil, okul politikasının ihlalini teşkil etmektedir ve idare onayıyla Disiplin Kurulu takibini gerektirir. İşbu politikaya veya politikanın belli bir duruma uygulanmasına ilişkin her türlü soru Namık Kemal Ortaokulu Bilgi Teknolojileri Direktörlüğü'ne ya da E-Güvenlik Koordinatörlüğü'ne iletilir.

- **GÖZDEN GEÇİRME**

Bu dokümanı gözden geçirme ve güncelleştirme sorumluluğu Bilgi Teknolojileri Direktörlüğü'ne aittir. Yapılan değişiklik ve güncellemeler idare onayıyla yayınlanır. Gözden geçirme her yıl Haziran ayında yapılır.

E-GÜVENLİK KOMİSYONU

Bülent Vural SAVAŞ (Müdür Yardımcısı)
Deniz YAPICI (Sosyal Bilgiler Öğretmeni
Merve EVCEN TEMELLİ (Bilişim Teknolojileri Öğretmeni
Seval İŞLEK (Rehber Öğretmen)
Serdar DOĞRU(Din Kültürü ve Ahlak Bilgisi Öğretmeni)

Mehmet Fahri ASLAN
OKUL MÜDÜRÜ