İSTİKLAL İLKOKULU YENİMAHALLE ANKARA

BU OKUL E-GÜVENLİK İNTERNET GÜVENLİĞİ PROTOKOLLERİNİ UYGULAMAKTADIR.
http://storage.eun.org/esafety-label-medal/Bronze_2021_1_en_fa6ac.png

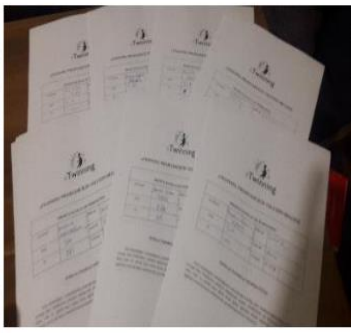
http://istiklalilkokulu.meb.k12.tr/

Okulumuzda öğrencilerimize e güvenlik anketi uyguladık. Öğrencilerimize e güvenlik ile ilgili videolar izlettik. Sonra esafety.eu sitesine üye olup dökümanları yükledik. Sonra anket sorularını cevapladık ve okulumuz eSafety Label – eGüvenlik Bronze etiket aldı.

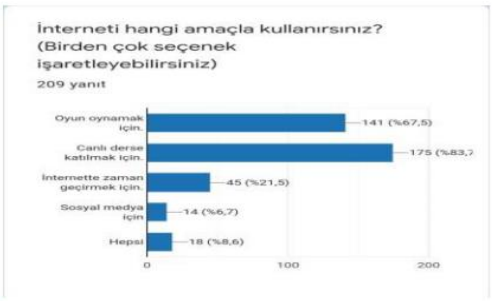
E-GÜVENLİK PANO ÇALIŞMAMIZ

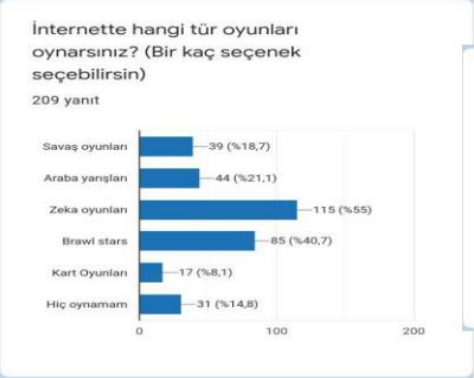
etwinning projesine dahil olan öğrenciler, ortak bir eGüvenlik panosu hazırladılar

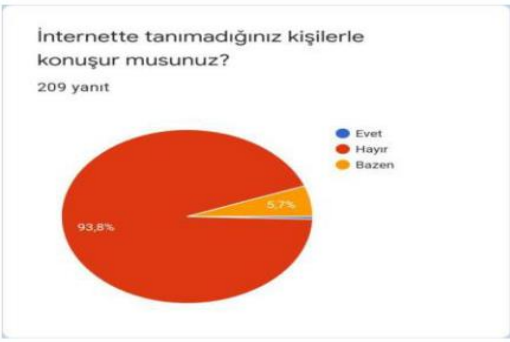
Our e-Security school board and parent permits !

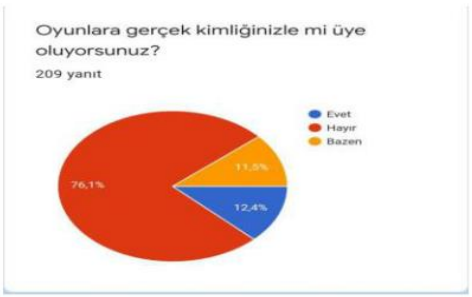


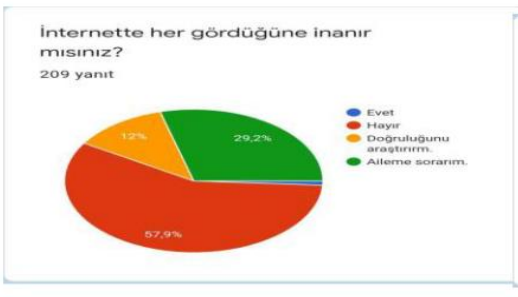
https://forms.gle/W2KJ9unSGRWiJ5bt9 *survey link*

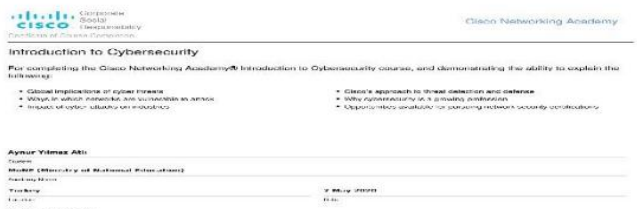












At our school, participation in eSafety Label related courses is provided.;

Etwinning projects are carried out in our school.& Swot Analysisi

GÜÇLÜ YÖNLER	ZAYIF YÖNLER	FIRSATLAR	TEHDİTLER
+Öğrencilerin ve velilerin ihtiyaç duyduklarında okul yönetimine, öğretmenlere ve rehberlik servisine kolayca ulaşabiliyor olması. +Akademik çalışmayı teşvik edici, yapıcı ve yönlendirici bir yönetim anlayışının olması. +Okul yönetimi ve çalışanlar arasındaki iletişimin sıcak ve güçlü olması. +Yönetici, öğretmen, öğrenci ve veli iletişiminin oldukça güçlü olması. +Yeniliklere açık ve gelişen teknolojiye uyum sağlayan, genç, dinamik ve başarılı bir okul kadrosunun olması. +Okulumuzda cep telefonu, fotoğraf makinesi ve benzeri teknolojik aletlerin izinsiz kullanılmaması ve bu kuralla ilgili görünür uyarı yazılarının bulunması. +Teknolojinin okul personeli tarafından yerinde ve doğru bir şekilde kullanılması ve derslerle bütünleşmiş olması.	-Salgın sürecinden dolayı sosyal ve kültürel faaliyetlerin yapılamaması. -Okulumuzda yeterince Teknik eleman bulunmaması. -Okulumuzda derslik dışında etkinlik yapılacak bir bölümün olmaması	+Okulumuzun bulunduğu konum itibariyle çevresinde başka okullarında bulunması nedeniyle veliler ve öğrenciler tarafından daha güvenli algılanması. +Ulusal ve Uluslar arası E-twinning Projelerinin yürütülmesi. +Okulumuzun E-Safety Label kapsamında etiket çalışmalarının yürütülmesi. Bu çalışmalar sonucu Bronz etiketin alınması	-Öğrencilerin teknoloji imkânlarını olumsuz yönde kullanma ihtimalinin olması. Öğrencilerin maddi imkansızlıklardan dolayı bilişim aletlerine ve internete yeterince ulaşamaması -Öğrencilerde cep telefonu, bilgisayar kullanma ve televizyon izleme alışkanlığının fazla olması. -İnternet tehditlerinin her geçen gün kendini yenilemesi ve daha cazip hale gelmesi

İSTİKLAL İLKOKULU OKUL POLİTİKASI

http://istiklalilkokulu.meb.k12.tr/

Okulda cep telefonu kullanımı hakkında öğrencilerimizin ve velilerimiz bilgilendirilmiştir. Ayrıca Okul web sayfasında bu yönetmelik paylaşılmış ve okul politikamızda da yer almıştır. Öğretmenler kurul toplasında da bununla ilgili kararlar alınmıştır.

İSTİKLAL İLKOKULU E-GÜVENLİK POLİTİKAMIZ HAKKINDA

• Çocuklarda bilinçli ve güvenli internet kullanımına dair bilgi, beceri ve tutumların geliştirilmesi için seminerler düzenlenmektedir.

• Ders müfredatlarına sosyal medya başta olmak üzere internetin bilinçli kullanımı ile ilgili konuların güncellenmesi sınıf öğretmenleri tarafından yapılmaktadır.

• Okulumuzda teknolojinin etkili ve güvenli kullanımlarının sağlanması için BTK tarafından güvenli internet ağı mevcuttur.

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

Aşağıda belirtilen siteler, veli toplantılarında, öğretmenler kurulu toplantılarında ve öğrencilerle yapılan seminerlerde tavsiye edilmektedir.

Daha Güvenli İnternet Merkezi (gim.org.tr) - Safer Internet Center'ın resmi sayfası.http://guvenlinet.org.tr/tr/

Güvenli Web (güvenli.web.org.tr) - çevrimiçi güvenlik konuları için farkındalık portalı.

Güvenli Çocuk (güvenli.cocuk.org.tr) - 13 yaşından küçük çocuklar için oyun ve eğlence portalı.

Ihbar Web (ihbar.web.org.tr) - yasadışı içerik için telefon hattı.

İnternet BTK (internet.btk.gov.tr) - İnternet ve BT yasası konusunda farkındalık portalı.

SID Page (gig.org.tr) - Güvenli İnternet Günü sitesi

FOTOĞRAF YA DA VİDEO ÇEKİMİ VE YAYINLANMASI

Bütün Veliler okula kayıt esnasında Web sayfasında ve eTwinning Projelerinde kullanılmak üzere öğrencilerin fotoğraf ve video çekimlerinden önce bir fotoğraf ve video izin formu imzalar. Okul idaresi tarafından görevlendirilen kişilerin çektiği fotoğraf ve videolar ancak Okulun resmi web adresinde ve sanal ortamlarında, ilgili öğrenci velisinin talep ve yazılı onayı ile yayınlanabilir

Öğrencisi için onay vermeyen velinin öğrencisi ile ilgili fotoğraf ve videolar yayınlanmaz.

Our students and parents were informed about the use of mobile phones at school. In addition, this regulation has been shared on the school website and has been included in our school policy. Decisions regarding this were also taken at the teachers' board meeting.

İSTİKLAL PRIMARY SCHOOL
ABOUT OUR E-SECURITY POLICY

• Seminars are organized to develop knowledge, skills and attitudes about conscious and safe internet use in children.

• Subjects related to the conscious use of the internet, especially social media, are updated in the curriculum by classroom teachers.

• Our school has a secure internet network by BTK to ensure effective and safe use of technology.

• Emphasis is placed on electromagnetic pollution and internet security in schools affiliated with the Ministry of National Education.

The sites listed below are recommended at parent meetings, teachers' board meetings and seminars with students.

Safer Internet Center (gim.org.tr) - The official page of Safer Internet Center.http: //guvenlinet.org.tr/tr/

Secure Web (secure.web.org.tr) - awareness portal for online security issues.

Safe Kids (Güvenlik.cocuk.org.tr) - Game and entertainment portal for children under 13.

Ihbar Web (ihbar.web.org.tr) - hotline for illegal content.

Internet BTK (internet.btk.gov.tr) - Awareness portal on Internet and IT law.

SID Page (gig.org.tr) - Safe Internet Day site

PHOTOGRAPHY OR VIDEO SHOOTING AND PUBLISHING

All Parents sign a photo and video consent form before the students take photos and videos to be used on the Web page during enrollment and in eTwinning Projects. The photographs and videos taken by the persons assigned by the school administration can only be published on the official web address and virtual environments of the School with the request and written approval of the relevant student's parent.

Photos and videos about the student of the parent who does not give consent for the student are not published.

Okulumuzda MEB'lığının yönergeleri takip edilmektedir.

MİLLÎ EĞİTİM BAKANLIĞI BİLGİ VE SİSTEM GÜVENLİĞİ YÖNERGESİ

BİRİNCİ BÖLÜM Amaç, Kapsam, Dayanak ve Tanımlar

Amaç

MADDE 1-(1) Bu Yönergenin amacı, Millî Eğitim Bakanlığı bünyesinde bulunan bilişim kaynaklarının kullanımına yönelik usul ve esasları belirlemektir.

Kapsam

MADDE 2-(1) Bu Yönerge, Bakanlık merkez ve taşra teşkilatındaki tüm personel ile kendilerine herhangi bir nedenle Bakanlık bilişim kaynaklarını kullanma yetkisi verilen paydaş ve konukları kapsar.

Dayanak

MADDE 3-(1) Bu Yönerge, 5/12/1951 tarihli ve 5846 sayılı Fikir ve Sanat Eserleri Kanunu, 26/9/2004 tarihli ve 5237 sayılı Türk Ceza Kanunu, 4/5/2007 tarihli ve 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun ile 25/8/2011 tarihli ve 652 sayılı Millî Eğitim Bakanlığının Teşkilat ve Görevleri Hakkında Kanun Hükmünde Kararname hükümlerine dayanılarak hazırlanmıştır.

Tanımlar

MADDE 4-(1) Bu Yönergede geçen;

a)Bakan: Millî Eğitim Bakanını,

b)Bakanlık: Millî Eğitim Bakanlığını,

c)Başkan: Bilgi İşlem Dairesi Başkanını,

ç)Başkanlık: Bilgi İşlem Dairesi Başkanlığını,

d)Bilişim Kaynakları: Elektronik ortamda yapılan iş ve işlemlerde kullanılan yazılım, donanım, araç ve gerecini,

e)Doküman Yönetim Sistemi (DYS) :Bakanlık elektronik belge yönetim sistemini,

f)ESHS: Elektronik Servis Hizmet Sağlayıcısını,

g)e-İmza: Başka bir elektronik veriye eklenen veya elektronik veriyle mantıksal bağlantısı bulunan ve kimlik doğrulama amacıyla kullanılan elektronik veriyi,

ğ)e-Okul: Bakanlığa bağlı okul/kurumlarda öğrenci ve yönetimle ilgili iş ve işlemlerin elektronik ortamda yürütüldüğü ve bilgilerin saklandığı sistemi,

h)e-Posta: İnternet üzerinden bilgisayarlar aracılığıyla bilgi alışverişini sağlamak için kullanılan elektronik haberleşme sistemini,

ı)e-Sınav Merkezi: Elektronik ortamda sınavların yapıldığı merkezi

i)Firma Personeli: Sözleşme, plan ve şartnamelere uygun biçimde bir işi/projeyi yapmayı üstlenen, bu amaçla işgücü, malzeme ve ekipman sağlayarak gerekli yöntemle istenen işi/projeyi tamamlamayı taahhüt eden resmî veya özel kurum veya kuruluş personelini,

j)Konuk: Bakanlık bünyesinde kullanmış olduğu bilgisayar, bilgisayar ağı, internet ve benzeri tüm bilişim sistemleri üzerinde yetkilendirilmemiş olan Bakanlık personeli dışındaki kişiler ile görev yeri dışında çalışan Bakanlık personelini, 2

k)Kullanıcı: Bakanlık bünyesinde yer alan bilgisayar, bilgisayar ağı, internet ve benzeri tüm bilişim sistemlerinden yararlanan tüm Bakanlık personeli ile Bakanlık bilişim kaynaklarını kullanma yetkisi verilen paydaş ve konukları,

l)Kurum: 652 Sayılı Kanun Hükmünde Kararname ve 6528 Sayılı Kanun'da yer alan Bakanlık

merkez teşkilatı ile İl/İlçe Millî Eğitim Müdürlükleri ile bu müdürlüklere bağlı örgün ve yaygın eğitim veren kurumları,
m)MEBBİS: Millî Eğitim Bakanlığı Bilişim Sistemlerini,
n)MEBNET: Bakanlık merkez ve taşra teşkilatı içerisinde yer alan tüm kurumlarda kullanılan intranet ve internet ağları (TTVPN, MEB İntranet, MEB ADSL, MEB VDSL, MEB Fiber, MEB FATİH Hattı, MEB Wimax, MEB Kamunet, MEB VPN, FATİH VPN, Kurumlararası VPN, MEB Mobil, MEB APN, MEB Uydunet, MEB Sanal Santral, e-Sınav Hattı vb. ağların tamamını) ile bilişim kaynaklarının tümünü,
o)Merkez: 652 Sayılı Kanun Hükmünde Kararname ve 6528 Sayılı Kanun'da yer alan Bakanlık merkez teşkilatı birimlerini,
ö)Paydaş: Ortak çalışma yapılan kurum veya kuruluşları,
p)Personel: Bakanlık merkez teşkilatı ile İl/İlçe Millî Eğitim Müdürlükleri ve bu müdürlüklere bağlı örgün ve yaygın eğitim veren kurumlardaki tüm çalışanları,
r)Sistem Odası: Bakanlık merkez teşkilatı, İl/İlçe Millî Eğitim Müdürlükleri veya e-sınav merkezlerinde bulunan sistem teçhizatının yer aldığı odayı,
s)Sistem Yöneticisi: Başkanlığımız uygulama ve sistemden sorumlu bilişim personeli ile İl/İlçe Millî Eğitim Müdürlüklerinde görev yapan MEBBİS Yöneticisi veya onun sorumluluğunda görev yapan bilişim personelini,
ş)Yüklenici Firma: Sözleşme, plan ve şartnamelere uygun biçimde bir işi/projeyi yapmayı üstlenen, bu amaçla işgücü, malzeme ve ekipman sağlayarak gerekli yöntemle istenen işi/projeyi tamamlamayı taahhüt eden resmî veya özel kurum veya kuruluşu,
ifade eder.

İKİNCİ BÖLÜM Sorumluluk ve Genel Kurallar

Sorumluluk

MADDE 5-(1) 5651 sayılı Kanun ve 27001 Bilgi Güvenliği Yönetim Sistemi kapsamında hukuki süreçlere kaynak teşkil etmesi ve sistemlerin güvenli bir şekilde işletilmesi amacıyla, Başkanlıkça uygun görülen sistemlerin, uygulamaların, kullanıcı işlemlerinin ve bilgi sistem ağındaki veri akışının iz kayıtları, ajanlı veya ajansız iz toplama yöntemleri kullanılarak toplanır ve ilgili kanun ve yönetmeliklerde belirtilen süre boyunca Başkanlıkça saklanır. Bu nedenle kullanıcı, kendisine ait kişisel verilerin gizli kalması ve korunması kaidesiyle, MEBNET ağı üzerinden gelen ve giden tüm trafik bilgilerinin önceden kullanıcıya haber verilmeksizin Başkanlık tarafından kayıt ve kontrol edilebileceğini, bu bilgilerin istatistik, raporlama ve inceleme amaçlı olarak kullanabileceğini bilir ve kabul eder.
(2) Bakanlık personelinin, çocukların cinsel istismarına, müstehcenliğe, şiddet ve intihara yönlendirmeye, uyuşturucu ve uyarıcı madde kullanımını özendirmeye yönelik internet sitelerine girmesi, sohbet oturumları açarak kuruma ait gizli bilgileri paylaşması, oyun oynaması, devlet büyüklerine hakaret etmesi; sosyal medya, gazete, forum ve benzeri sitelerde kurumu küçük düşürücü ve kamuoyunu yanıltmaya yönelik yorumlar yapması, özel hayatına ilişkin suç oluşturabilecek nitelikteki bilgi ve işlemleri kurum internet hattı üzerinden yapması ile ilgili cezai ve hukuki sorumluluğu kendisine aittir. Başkanlık yukarıda belirtilen davranışları tespit etmeye ve önlemeye yönelik erişim politikaları belirler ve uygular.

(3) Bu Yönerge kapsamında bilgi ve sistem güvenliğinin planlı, sorunsuz, güvenli ve disiplin içinde gerçekleştirilmesinden Bakanlık bilişim sistemlerinden yararlanan tüm Bakanlık personeli birinci derecede görevli ve sorumludur. Bu Yönerge kapsamında olup teknolojik değişikliklere ya da Bakanlığın genel politikasındaki ve hizmetlerindeki değişikliklere göre bu politikada gerekli

düzenlemeler Başkanlıkça yapılır ve resmî internet sayfasında "Bilgi ve Sistem Güvenliği Politikaları"' adı altında yayımlanır. Tüm Bakanlık personeli yayınlanan "Bilgi ve Sistem Güvenliği Politikaları" nı takip etmekle ve bu politikalara uymakla yükümlüdür.
3

(4) Başkanlık, yasal hükümler çerçevesinde bilişim kaynaklarını ve bunlarla gerçekleştirilen aktiviteleri izleme, kaydetme ve periyodik olarak inceleme ve denetleme hakkını saklı tutar.
(5) Bakanlık bilişim kaynaklarında meydana gelen arızalara yetkisiz personel tarafından müdahale edilemez. Edilmesi sonucunda teknik destek verilmez ve ortaya çıkabilecek arızalar, maddi hasarlar ya da kurumsal ağ güvenliğinin ihlaline yol açan uygulamalardan ilgili personel sorumludur.
(6) Bakanlık demirbaşına kayıtlı olmayan, personelin şahsi bilgisayarlarına arıza bakım ve teknik destek hizmeti sunulmaz.
(7) Veritabanı yöneticileri tarafından MEBBİS, e-okul ile diğer bilişim modüllerinden yapılan tüm sorgular kayıt altına alınır. Başkanlık gerek gördüğü zaman sorgulamanın sebebini kullanıcıya yazılı veya sözlü olarak sorar. Yetkili kullanıcı hesabında anormal sorgu durumları tespit edilmesi durumunda hesap sahibine haber verilmeye gerek duyulmadan hesabı dondurup gerekli inceleme ve soruşturma işlemini başlatabilir.
(8) Merkez teşkilatı, taşra teşkilatı ile okul ve kurumlarda bulunan yetkili kullanıcı hiçbir sebepten ötürü öğretmen, öğrenci ve velilere ait kişisel bilgileri (ad soyad, T.C. kimlik numarası, çalıştığı kurum, okuduğu okul, adres, telefon numarası, e-posta adresi vb.) diğer kamu kurumları ve 3. şahıslar ile paylaşamazlar. Gerekli görüldüğü zaman bu bilgilerin paylaşımı için Başkanlıktan talepte bulunurlar. Başkanlık uygun gördüğü durumlarda bilgileri yasal sınırlar içerisinde ilgili kamu kurum ve kuruluşları ile paylaşır.
(9) Kullanıcı, kurumun kritik bilgisinin ortaya çıkmasına veya kurum servislerinin ulaşılmaz hale gelmesine sebep olabilecek tüm eylemlerden kaçınır.
(10) Kullanıcı, kullanımına tahsis edilen bilişim kaynaklarının güvenliğine yönelik önlemleri alır.
(11) MEBNET ağı ve bu ağı kullanan her kullanıcı ve cihaz ile ilgili her türlü erişim, güvenlik ve yönetim politikaları Başkanlık tarafından belirlenir ve uygulanır. Bu ağ üzerindeki trafik, ilgili erişim kanunu çerçevesinde gelen ve giden yönünde kayıt edilip incelenebilir ve raporlanabilir.
(12) Başkanlık, gerekli durumlarda Bakanlık Makamınca belirlenen erişim politikası düzenlemelerini uygular.

Genel Kurallar
MADDE 6-(1) Kullanıcı, bilgi teknolojileri kapsamındaki bilişim kaynaklarına zarar veremez, işleyişi aksatma, yavaşlatma veya durdurma eylemlerinde bulunamaz, içeriğini izinsiz olarak değiştiremez.
(2) Kullanıcı, bilgi teknolojileri kapsamındaki herhangi bir kaynağı, kendisinden başka hiç kimse adına ve yararına kullanamaz veya bir başkasının kullanımına izin veremez.
(3) Kullanıcı, başka kullanıcıların bilgisayarında yer alan şifrelendirilmiş paylaşım alanlarına çeşitli yöntemleri kullanarak erişemez ve bu türlü girişimlerde bulunamaz.
(4) Kullanıcı, çalışmalarının sonlandırılması ile birlikte kendisinde bulunan bilgisayar, yazıcı, disk ve benzeri tüm donanım ve malzemeleri, tüm yazılım ürünleri ve kodları ile bilişim sistemleri kullanımına yönelik tüm şifreleri içeren Bakanlığın tüm bilişim varlıklarını iade eder. Kullanıcının bilgi ve bilgi işleme olanaklarına erişim hakları kaldırılır.

(5) Yüklenici firma personeli, ancak sistem yöneticisi nezaretinde ve kontrolünde çalışma yapar. Firma personeli tarafından yapılacak çalışmalara nezaret edecek kurum personeli, en az firma personeli kadar konusunda uzman personel arasından seçilir ve sistem yöneticisinin onayı ile kayıt altına alınır. Bu kurallara uyulmadığı zaman doğacak problem ve zararlardan ilgili yüklenici firma sorumludur. Nezaret eden kurum personeli yapılan çalışmaları kayıt altına alır ve herhangi bir olumsuzluk durumunda bu olumsuzluğu açıklayıcı rapor sunmak zorundadır.
(6) Bilgi güvenliğini etkileyen arızalar mümkün olan en kısa sürede uygun yönetim kanalları kullanılarak Başkanlığa rapor edilir.
(7) Gizlilik içeren bilgiler ile kişisel veriler, e-devlet kapsamında protokol yapılarak bilgi paylaşımı yapılan veya kanunen yetkili sayılan merciler dışında hiçbir kişi, kurum ya da kuruluş ile paylaşılmaz.
(8) Gizlilik içeren bilgilerin paylaşımı ile ilgili yapılacak protokoller Bakanlık merkez birimlerince veya Bakanlıkça yetkilendirilen taşra teşkilatı birimlerince yapılır. 4

ÜÇÜNCÜ BÖLÜM Bilgi ve Sistem Güvenliği Kuralları ve Politikaları

Aktif Dizin Hizmetleri Kuralları

MADDE 7-(1) Bakanlık ve İl Millî Eğitim Müdürlüğü bünyesinde çalışmakta olan veya işe başlayan her personel ile paydaş ve konuklar için aktif dizin kullanıcı hesabı açılır. İl Millî Eğitim Müdürlüklerinde geçici süreliğine görevlendirilen paydaş ve konukların kullanımı için bağlı oldukları birimde görev yapan şef veya yetkili personel adına profili ve şifresi farklı ilave kullanıcı hesapları açılır. Geçici görevli personel bu hesaptan sorumludur. Geçici görevli personelin görevlendirme süresinin sonunda ilgili hesabın şifresi değiştirilir ve bir sonraki kullanıma kadar pasif halde bekletilir.
(2) Kullanıcı, kendisine verilen "kullanıcı adı"nı ve "şifresi"ni bir başkası ile paylaşmaz ve bir başkasına kullandırmaz. Kullanıcının, "kullanıcı hesabına" ait geçici şifresini derhal değiştirerek, bu Yönergenin 9'uncu maddesinde yer alan şifre politikasına uygun olarak şifresini oluşturur.
(3) Kullanıcının, Başkanlıkça belirlenecek periyodlarla "kullanıcı şifresini" değiştirmesi gerekir. Kullanıcı şifresini yenilemeyen veya kullanıcı şifresini üst üste birkaç kez hatalı giren kullanıcının, kullanıcı hesabı geçersiz kılınır ve iletişim ağına giriş izni otomatik olarak kaldırılır. İlgililerin başvurması halinde ilgili hizmetin bir üst yetkilisi tarafından uygun görülenler tekrar aktif hale getirilir.
(4) Her bir kullanıcı, bilgisayarda kendi "kullanıcı adı" ve "şifresi" ile oturum açarak çalışır. Çalışması biten kullanıcı, oturumu veya bilgisayarını kapatarak bilgisayara başkalarının fiziksel erişimini engeller. Bilgisayar başından kısa süreli ayrılmalarda bilgisayar oturumunu kilitler.
(5) İlgili hesabın amacı dışında kullanılması ve bu hesaptan doğabilecek zararların sorumluluğu, hesabı kullanan kullanıcıya aittir.
(6) Bakanlık ve İl Millî Eğitim Müdürlüğü'ndeki her bir son kullanıcı ve bilgisayar etki alanı üyesi olmalıdır. Etki alanında olmayan kullanıcı veya bilgisayarın internet erişimleri engellenir.

e-Posta İşlemleri Kuralları

MADDE 8-(1) Kullanıcı, tüm resmî yazışmalarında e-posta adresi olarak, Başkanlıkça kendisine tahsis edilen veya çalıştığı birime ait olan kendisine zimmetli e-posta adresini kullanır. Bunun dışındaki e-posta servislerini resmî işlerde kullanılmaz.
(2) Kullanıcı, kurum saygınlığını zedeleyecek ve/veya başkalarını taciz edecek kurum içi veya kurum dışı e-posta gönderemez. e-Posta adresini internet üzerinde herhangi bir siteye kurumsal amaçlar dışında abone olmak için kullanılamaz.

(3) Kullanıcı, Başkanlık tarafından kendisine veya çalıştığı birime tahsis edilen e-posta adresini, sohbet (chat) yapmak için kullanmaz.
(4) Kullanıcı, hesabını ticari ve kar amaçlı olarak kullanamaz. Çok sayıda kullanıcıya toplu halde reklam, tanıtım, duyuru ve benzeri amaçlı e-posta gönderemez ve zincir e-posta, sahte e-posta ve benzeri zararlı e-postalara yanıt yazamaz.
(5) Kaynağı bilinmeyen e-posta ekinde gelen dosyalar kesinlikle açılmaz ve derhal silinir.
(6) Kullanıcı, kendisine ait e-posta adresinin şifresinin güvenliğinden ve gönderilen e-postalardan doğacak hukuki işlemlerden sorumludur. Şifresinin başkası tarafından tespit edildiğini fark ettiği anda şifresini değiştirip Başkanlıkla temasa geçip durumu haber vermekle yükümlüdür.
(7) Güvenlik ve performans açısından e-posta eklentilerinin toplam boyutu hiç bir durumda Başkanlığın belirlediği boyut değerinden fazla olamaz.
(8) e-Posta hesapları için öngörülen kotadan dolayı bir problem yaşamaması için e-posta hesabının kontrolü kullanıcıya aittir.
(9) Resmî işler için Bakanlığın resmî e-posta hesapları dışında hiçbir e-posta adresine veri toplanamaz. Bu e-postalara cevap verilmez.
(10) Başkanlık sistem ve kullanıcı güvenliğini sağlamak amacıyla gelen giden e-postalar için politika belirleyebilir ve uygulayabilir. 5

(11) Başkanlık kişisel verilerin korunması ve gizli kalması kaidesiyle gelen giden e-postalara ait istatistiki bilgileri kayıt edebilir ve inceleyebilir.
(12) Gerekli görülmesi halinde Başkanlık kullanılan e-posta sistemleri üzerinde her türlü değişikliği yapma hakkına sahiptir.
(13) Bakanlık personeli olma vasfını kaybedenlerin (emeklilik, istifa, kurum değişikliği, vefat, işten çıkarılma vb.) isimleri ilgili birim tarafından Başkanlığa bildirilir. Başkanlığın belirlediği süre sonunda bu e-posta hesapları silinir.
(14) Usulsüz kullanıldığı tespit edilen veya spam, virüs yayarak sistem ve kullanıcıların güvenliğini tehdit eden e-posta hesapları devre dışı bırakılır. Kullanan hakkında gerekli yasal işlem başlatılır.
(15) Bakanlık birimlerinin talebiyle oluşturulan e-posta gruplarının üyelerinin güncel olmasından ilgili birim sorumludur. Birimin kapanması, isminin değişmesi, faaliyetin bitmesi vb. nedenlerle işlevini kaybeden e-posta grubunun kapatılması veya grup üyelerinde ekleme, çıkarma yapılması taleplerini Başkanlığa bildirir.

Şifre Politikası

MADDE 9-(1) Kullanıcı, kurumda kullanılan ve belirli bir şifre ile girilmesi zorunlu olan her türlü uygulama için şifre belirler.
(2) Kullanıcının şifrelerini belirlerken dikkat edeceği kurallar şunlardır:
a) Şifreler en az 8 (sekiz) karakter olmalıdır.
b) Şifreler küçük harf, büyük harf, rakam ve simgelerin kullanıldığı karışık yapıda olmalıdır**.**
c) Şifrelerin Başkanlıkça belirlenecek sayıda hatalı girilmesi sonucu, kullanıcı hesabı Başkanlığın politikalarına bağlı olarak kilitlenebilir. İlgililerin başvurması halinde ilgili hizmetin bir üst yetkilisi tarafından uygun görülenler tekrar aktif hale getirilir.
ç) Şifreler en geç altı ayda bir değiştirilir.
d) "Yönetici/Admin" kullanıcı şifreleri sadece sistem yöneticilerinde olur, kesinlikle son kullanıcılarla ve yüklenici firmalarla çalışıldığı zaman firma personeliyle paylaşılmaz.
e) Şifreler herhangi bir kişi ile paylaşılmaz.

Temiz Masa - Temiz Ekran Politikası

MADDE 10-(1) Sistemlerde kullanılan şifreler, masaüstü veya ekran üstü gibi herkes tarafından görülebilecek yerlere yazılmaz.
(2) Personel, bilgisayarını belli bir süre kullanmadığı zaman otomatik olarak şifre ile oturum açmasını gerektirecek şekilde ayarlar.
(3) Kullanıcı, gizli bilgi içeren evrakı ağ üzerinden paylaşmaz, gizli bilgi içeren atık evrakı imha eder.
(4) USB bellek, harici disk vb. hafıza ünitelerinin kullanım şartlarını Başkanlık belirler. Başkanlık gerekli gördüğü durumlarda ilgili ünitelerin kullanımının durdurulması, sınırlandırılması veya kriptolanması/şifrelenmesi gibi uygulamaları yürürlüğe koyar.
(5) Personel, bilgisayarındaki, USB belleğindeki, harici diskindeki ve benzeri veri depolamanın mümkün olduğu ortamlardaki gizlilik dereceli bilgi içeren her türlü belgenin güvenliğini sağlamakla yükümlüdür. USB veya harici diske gizli/önemli verilerin konulması gerekiyorsa kriptolanarak/şifrelenerek saklanır.

Ağ ve İnternet Kullanımı
MADDE 11-(1) Tüm kullanıcılar interneti bilinçli bir şekilde kullanmak, başkalarının hakkını ihlal edici ve bilişim sisteminin işleyişini engelleyici, bozucu faaliyetlerde bulunmamakla yükümlüdür.
(2) Kullanıcı;
a) Bakanlık sunucuları üzerinde kendisine tahsis edilen kullanıcı adı, şifre ve IP adresi kullanılarak gerçekleştirilen her türlü etkinlikten, 6

b) Kendisine tahsis edilen bilgisayar üzerinde bulundurduğu belge, yazılım gibi her türlü kaynağın içeriğinden,
c) Bilişim sisteminin kullanımı hakkında yetkili makamlar tarafından talep edilen bilgilerin doğru ve eksiksiz verilmesinden,
ç) Bakanlık tarafından sağlanan güvenlik programlarının aktif olarak kullanılmasından ve güncellenmesinden,
d) Bilişim sisteminin; kullanım kurallarına, kanun ve yönetmelikler ile Bakanlığın tabi olduğu mevzuata uygun olarak kullanımından
sorumludur.
(3) Kullanıcı, Bakanlık merkez ve taşra teşkilatı bünyesindeki tüm bilişim kaynaklarını ve MEBNET'i;
a) Bakanlık ağına ve haricindeki bir sisteme, ağ kaynağına veya servisine saldırı niteliğinde girişimlerde bulunmak,
b) Diğer kullanıcılara ait verileri bozmak ya da zarar vermek, gizlilik hakkını ihlal etmek,
c) Yasaklanmış her türlü materyali üretmek ya da dağıtmak,
ç) Gerçek dışı, sıkıntı ve rahatsızlık verici, gereksiz endişe yaratacak materyali üretmek ve dağıtmak,
d) Başka bir kullanıcının e-posta adresini, o kullanıcının izni olmadan kullanmak,
e) Yerel, ulusal, uluslararası bilgisayarları veya hizmetleri kasıtlı olarak yetkisiz kullanmak,
f) Başkalarının telif haklarını ihlal edici konumda olan yazı, makale, kitap, film, müzik eserleri gibi materyali edinmek, yayınlamak, dağıtmak,
g) Özel yazılım, oyun, film, müzik, video vb. materyalleri edinmek, yayınlamak, kullanmak, dağıtmak,
ğ) Canlı televizyon ve radyo yayınlarını izlemek/dinlemek,

h) Resmî işlemler dışındaki interaktif uygulamalara/hizmetlere erişmek,
ı) Bulut ve depolama sistemlerine erişmek,
i) Sosyal medya hesaplarına erişmek,
j) Siyasi ve ideolojik propaganda yapmak
için kullanamaz.
(4) Telif hakları ve lisansları ihlal eden, zararlı yazılım bulunduran, MEBNET ağında yoğun ağ trafiğine sebep olan iki veya daha fazla kullanıcı arasında veri paylaşmak için kullanılan noktadan noktaya (Peer-to-peer - P2P) uygulamaları kullanılmaz. Dosya paylaşımı, anlık mesajlaşma programları ve kurum altyapısında soruna yol açacak şekilde yoğun ağ trafiğine sebep olan uygulamalar ile güvenlik tehdidi oluşturan reklam, içerik, site, kullanıcı, yazılım, uygulama, erişim sağlayan cihazların tamamı gerekli görüldüğünde Başkanlık tarafından filtrelenir veya erişime kapatılır.
(5) Zararlı veya güvenlik tehdidi oluşturan yazılım, uygulama, eklenti vb. içerik barındıran bilgisayarlar yeniden kurulum yapılmadan kurumsal ağa dâhil edilemez.
(6) Bilgisayarlara tahsis edilen IP numarası ve ortam erişim kontrolü adresi (MAC adresi) ile BIOS ayarları Bakanlık tarafından yetkilendirilmiş kişiler dışında değiştirilemez.
(7) Kurum ağına sistem yöneticisinin bilgisi dışında herhangi bir aktif ağ cihazı eklenemez.
(8) Kullanıcılar, kişisel bilişim kaynaklarını kurum ağında sistem yöneticisinden izin almadan kullanamaz.
(9) Kurum içinde hizmet veren sunucu, sistem veya kullanıcı bilgisayarlarına uzaktan erişim, zorunlu hallerde Başkanlığın onayı/izni alınarak yapılır.
(10) MEBNET erişimleri ve kaynakları öncelikli olarak resmî ve onaylı kurum işlerinin gerçekleştirilmesi için kullanılır. 7

(11) Başkanlık gerekli gördüğü durumlarda kurum içi kritik düzeydeki hizmetlere (MEBBİS, e-okul, DYS vb.) öncelik sağlamak için MEBNET ağında bant genişliği düzenleme yoluna gidebilir.
(12) MEBNET ağında kategorisi olmayan ip adresi, içerik veya sitelere erişim izni verilmez. Erişim talepleri Yardım Masası Modülü (yardimmasasi.meb.gov.tr) üzerinden yapılır.
(13) Başkanlık gerekli gördüğü durumlarda eğitim, devlet, pedagoji kategorileri dışında kalan kategorilere yönelik erişimi düzenleme hakkına sahiptir.
(14) Kullanıcı, kendi kullanıcı hesaplarıyla internet üzerinden gerçekleştirdiği tüm işlemlerden sorumludur. Kimlik bilgilerini uygun bir şekilde saklar ve başkalarıyla paylaşmaz.
(15) Kurumsal ağ güvenliği açısından tehlike yaratabilecek nitelikte zararlı olduğu tespit edilen internet adreslerine erişim tüm kullanıcılar için engellenir. Kullanıcı bu tür engellemelerin kaldırılması konusunda Başkanlıktan herhangi bir talepte bulunamaz.
(16) Kurumsal ağ üzerindeki bilgisayarlara erişim hakkı, yetkisi olmayan kişilere verilemez.
(17) Yetkilendirilmiş kişiler ve kuruluşlar dışında, ağ kaynağına veya servisine zarar verebilecek DOS saldırısı, port/ağ taraması, paket dinleme, ağ izleme, IP değiştirme gibi kasıtlı veya kasıtsız girişimlerde bulunamaz.
(18) Bakanlık merkez ve taşra teşkilatında tanımı Başkanlık tarafından yapılan MEBNET ağı dışında bir ağ kullanılamaz. Kullanıcı Bakanlık merkez ve taşra teşkilatında bulunan bilgisayarlardan MEBNET ağı dışında cep telefonu, ADSL, VDSL, fiber, mobil modem, kişisel erişim noktası, kablosuz bağlantı alanı cihazı vb. cihazlarını kullanamaz.
(19) Bakanlık merkez ve taşra teşkilatında MEBNET ağında Başkanlık tarafından oluşturulan MEB Sertifikası kullanılır. MEB Sertifikası yüklü olmayan cihazların erişimine izin verilmez.
(20) Merkez ve taşra teşkilatında MEBNET ağına izinsiz kablosuz bağlantı alanı cihazı takılamaz.

İzin dahilinde takılan kablosuz bağlantı alanı cihazları şifresiz kullanılamaz.
(21) Kurum bilişim kaynakları; ağ ve internet kaynaklarının kurum dışından kullanılmasına sebep olabilecek ya da kurum dışındaki kişi ya da bilgisayarların kendilerini kurum içerisindeymiş gibi tanıtmalarını sağlayacak (DHCP, DNS, Proxy, IP Sharer, NAT vb.) şekilde kullanılamaz.
(22) Başkanlık MEBNET ağında erişime açılacak ve kapanacak portları belirleme ve düzenleme yetkisine sahiptir. Uzaktan erişim (rdp, ssh, telnet vb.), dosya-yazıcı paylaşımı gibi portlara ve uygulamalara erişim izni verilmez. MEBNET ağında TCP/FTP (21), TCP/HTTP (80), TCP/HTTPS (443) portlarına erişim önceliği verilir. e-Sınav merkezlerinin ağı kapalı devre olup; internet erişimine kapalıdır.
(23) Bakanlığa ait gizli ya da açık her türlü veri Bakanlık sistemleri üzerinde barındırılır. Herhangi bir bulut depolama sistemine veri aktarılmaz.
(24) Kurumsal ağ üzerindeki bilgisayarlarda güvenlik politikalarının Başkanlık tarafından belirlendiği antivirüs yazılımının kullanılması zorunludur.
(25) Başkanlığın mevcut anket programı hariç anket programları veya formlar veri toplama ve depolama amacıyla kullanılamaz.
(26) Bakanlık bilişim kaynaklarında ve MEBNET ağında zararlı yazılım tespit edilen, saldırmaya yönelik teşebbüste bulunan ve kullanılan güvenlik sistemlerini aşmaya, atlatmaya yönelik her türlü tünel, proxy, vpn vb. program kullanan kullanıcı veya kurumların, internet ve intranet erişimleri kesilir. İlgili durum ortadan kalkınca erişim tekrar sağlanır. Erişim politikalarını ve sistemlerini aşmaya veya bilişim sistemlerine saldırmaya yönelik girişimde bulunan kullanıcı veya kurum hakkında yasal işlem başlatılır. Ayrıca Bakanlık sistemlerine yönelik dışarıdan vpn, proxy, tünel vb. bağlantılarla erişim sağlanması (kullanıcının kendi ip adresi yerine sahte ip adresleri üzerinden erişmesi), saldırı girişiminde bulunulması durumunda ilgili erişimler engellenir. Erişim kesintileri ile ilgili süreçler Başkanlık tarafından belirlenir ve yönetilir.
(27) Başkanlığın onayı olmadan hiçbir yazılım satın alınamaz. Satın alınması düşünülen yazılım ve programlar için Başkanlıktan uygun görüş alınır.

Sanal Santral Hizmetleri

MADDE 12-(1) Merkez ve taşra teşkilatında Başkanlığın izni olmadan voip, ip santral, faks, telsiz telefon, analog telefon vb. hizmetler kullanılamaz. 8

(2) Sanal santral ile ilgili telefon talepleri hariç;
a) Telefon üzerindeki tanımlamanın değiştirilmesi,
b) Telefon arama yetkilerinin düzenlenmesi,
c) Telefon numarasının değiştirilmesi,

ç) Telefon ve ek modül üzerindeki hızlı arama kayıtlarının eklenmesi ve güncellenmesi,
d) Çağrı yönlendirme ve numara engellemesi,
e) Yönetici telefonlarını doğrudan arayacak numaraların oluşturulması ve güncellenmesi,
f) Telefon ve faks arızalarının bildirilmesi,
g) Çağrı toplama talepleri,
ğ) Telefonların yer değiştirmesi,
h) Çağrı dökümü ve kullanım bilgileri
ile ilgili talepleri bağlı bulunduğu genel müdürlüğün ve/veya başkanlığın kurumsal e-posta adresi ya da DYS üzerinden resmî yazı ile Başkanlığa yapılır. Talepler Başkanlığın onayından sonra gerçekleştirilir.

(3) Personel, kurum telefonunu özel işleri için kullanamaz.
(4) Sanal santral hizmetlerinin yürütülmesi Başkanlık tarafından yapılır.

Sistem Odası Güvenliği

MADDE 13-(1) İl/İlçe Millî Eğitim Müdürlükleri ve e-sınav merkezlerinde yer alan sistem odaları ilk kurulumda binanın durumuna göre Bilgi İşlem ve Eğitim Teknolojileri Şube Müdürlüğü ile yanyana merkezi bir lokasyonda tercih edilmeli ve kurulmalıdır. Sistem odasının üstünde ıslak zeminli (tuvalet, banyo vb.) oda bulunmamalıdır. Kurulumda jeneratör, kesintisiz güç kaynağı, klima ile yangın, duman, nem ve su sensörlü algılama-önleme sistemleri tercih edilmelidir. Mevcut kurulu sistem odaları yukarıda belirtilen niteliklere göre iyileştirilmelidir. Sistem odalarının giriş ve çıkış kapılarında gerekli güvenlik önlemleri (kilit, şifre, parmak izi, kamera vb.) alınmalıdır. Sistem yöneticisinin bilgisi ve izni dışında giriş çıkışlar yapılmamalıdır. Giriş çıkışlar kayıt altına alınmalıdır.
(2) Sistem odasında gürültü ve titreşime karşı yalıtım önlemi sağlanmalıdır. Bakım, kontrol ve acil durum çizelgeleri görünür bir panoda yer almalıdır. Sistem odasının periyodik olarak kontrolleri sağlanmalı ve ilgili çizelgelere işlenmelidir.
(3) Sistem odasında kesintisiz güç kaynağı ile soğutma sistemleri aktif olarak çalışmalıdır. Sistem odasında meydana gelen arıza vb. durumlarda Başkanlığa bilgi verilerek en kısa sürede arızanın giderilmesi sağlanmalıdır.
(4) Bakanlık merkez ve taşra teşkilatında yer alan sistem odalarının tasarım ve işletme süreçleri Başkanlık koordinasyonunda yapılmalıdır.

İnternet Sitesi Barındırma Hizmeti Politikası

MADDE 14-(1) Bakanlığımız kurumları ile Bakanlığımız sorumluluğunda yürütülen projelere ait internet sitelerinin barındırma hizmeti Bakanlık sunucuları üzerinden yapılır.
(2) İletişim için kurum tüzel kişiliğine ait e-posta adresi kullanılır.
(3) Başkanlığın onayı olmadan alan adı alınamaz. Bakanlığa ait olmayan sunucularda web hizmeti yayını yapılamaz, dosya ve veritabanı depolanamaz. Alan adı alınması gereken durumlarda Başkanlıktan onay alınır ve onayı müteakip http://moduller.meb.gov.tr adresine proje olarak kaydedilir.
(4) Kurum internet sitelerinin hazırlanmasında, güncellenmesinde ve yönetilmesinde dikkat edilecek hususlar şunlardır:
a) Bakanlık tarafından belirlenen internet sitesi standartlarına göre hazırlanır.
b) Her türlü içerikten kurum amiri sorumludur.
c) Uygulamalara yetkisiz kişilerin erişimini engelleyen tedbirler alınır. 9

ç) Alınan web hizmetine ait şifreler kurum amiri ve görevli personelin sorumluluğu altındadır.
d) Kritik öneme sahip içerikler web hizmeti alan kurum tarafından görevlendirilen yetkili ya da yetkililerce güvenli bir ortamda yedeklenir.
e) Herhangi bir saldırı halinde site üzerinde bir değişiklik yapılmadan Başkanlığa haber verilir.
f) Tahsis edilen web alanında virüs, truva atı vb. zararlı içerik veya bağlantı, oyun, yetkisiz erişime sebep olabilecek uygulamalar bulundurulmaz.
g) Yayınlanacak her türlü içerik telif hakları, fikrî haklar, şeref ve haysiyetin korunması ve gizlilikle uyumlu olur.
ğ) Bakanlığın herhangi bir politikasını, kuralını ya da düzenlemesini ihlal edemez.
h) Web barındırma alanı, internet sitesi yayıncılığı dışında dosya depolama ya da arşiv alanı olarak kullanılamaz.

Nitelikli Elektronik Sertifika (e-İmza) Kullanımı

MADDE 15-(1) Bakanlığımız Elektronik Belge Yönetimi, Doküman Yönetim Sistemi üzerinden güvenli elektronik imza ile yapılır.

(2) Güvenli elektronik imza sayısal imzadır ve elle atılan imza ile aynı hukukî sonucu doğurur ve aynı ispat gücüne haizdir.

(3) Kullanıcılar elektronik imzalarını ve şifrelerini hiçkimse ile paylaşmaz.

(4) e-İmza veya şifrenin başkasının eline geçmesi sonucu meydana gelecek her türlü durumda yasal sorumluluk e-imza sahibine ait olur.

(5) e-İmzanın çalınması, kaybedilmesi durumunda sorumluluk kullanıcıya aittir ve ESHS'den temin eder.

(6) Kullanıcı sertifika sağlayıcılarından gelen e-imza güncellemelerinin tarihlerini takip eder ve güncellemeleri zamanında, e-imzasını kullanarak yapar. Aksi takdirde ortaya çıkabilecek her türlü maddi ve hukuki sonuçtan sertifika sahibi sorumludur.

(7) Kullanıcı, ESHS'ye tanımlı kişisel bilgi değişikliklerini ESHS' ye bağlı çağrı merkezlerini arayarak günceller.

Yaptırım ve Uygulama

MADDE 16-(1) Başkanlık, bilişim kaynaklarının yönergeye aykırı etkinlikler dahilinde kullanılması durumunda; gerçekleştirilen eylemin; yoğunluğuna, kaynaklara veya kişi/kurumlara verilen zararın boyutuna ve tekrarına göre aşağıdaki işlemlerin bir ya da birden fazla maddesini, sıra ile ya da sırasız uygulayabilir;

a) Kullanıcı sözlü veya yazılı olarak bilgilendirilir.

b) Kullanıcıya tahsis edilmiş kurum bilişim kaynakları sınırlı veya sınırsız süre ile erişime kapatılır.

c) Yönergeye aykırı kullanım halinde kullanıcı hakkında gerektiğinde idari ve adli soruşturma açılması için gerekli işlemler başlatılır.

DÖRDÜNCÜ BÖLÜM Çeşitli Hükümler

Hüküm Bulunmayan Hususlar

MADDE 17-(1) Bu Yönergede hüküm bulunmayan hususlarda ilgili diğer mevzuat hükümlerine göre işlem yapılır.

Yürürlük

MADDE 18-(1) Bu Yönerge onaylandığı tarihte yürürlüğe girer.

Yürütme

MADDE 19-(1) Bu Yönerge hükümlerini Millî Eğitim Bakanı yürütür.

Yürürlükten Kaldırma 10

MADDE 20-(1) 11/04/2012 tarihli ve 565 sayılı Makam Olur'u ile yürürlüğe giren Bilgi ve Sistem Güvenliği Yönergesi bu Yönergenin yürürlüğe girdiği tarihte yürürlükten kalkar.

İSTİKLAL İLKOKULU MÜDÜRLÜĞÜ

2020/2021 EĞİTİM ÖĞRETİM YILI

eTWİNNİNG ÖĞRETMENLER KURULU TOPLANTI TUTANAĞI

Toplantı Tarihi ve Saati **:** 08/01/2021

Toplantı No: 1

GÜNDEM MADDELERİ

1. Açılış ve Yoklama
2. eTwinning portalının öğretmenlere tanıtılması ve üye olmalarının sağlanması
3. eTwinning online eğitim sitesinin tanıtılıp eTwinning eğitimlerine katılımın teşvik edilmesi
4. e Güvenlik uygulamaları ve müfreadata entegrasyonu
5. Öğretmenlerin rehber öğretmenler tarafından verilen e bağımlılık,e güvenlik ve bilinçli internet kullanımı eğitimlerine ve e güvenlikle ilgili EBA online eğitimlere MEB Hizmetiçi eğitim faaliyetlerine katılımın teşvik edilmesi
6. Okulda taşınabilir cihaz ve cep telefonu kullanımı
7. Okul politikasının oluşturulması
8. Okulda yürütülen eTwinning projelerinin tanıtılması
9. eTwinning okulu çalışmalarının desteklenmesine
10. Kapanış

ALINAN KARARLAR:

1. eTwinning portalının ve eSafety portalının bütün öğretmenlere tanıtımı yapıldı.Öğretmenlerin her iki portala da üye olmalarına karar verildi.
2. eTwinning online eğitim sitesinin tanıtımı yapıldı.Bütün öğretmenlerimizin yapılan eğitimleri takip ederek katılım sağlamalarına karar verildi.Ayrıca ilçe-il-ülke geneli yapılan eğitimlere de katılımın sağlanmasına karar verildi.Eğitim duyurularının okul idaresi ve öğretmenler tarafından takip edilmesine ve duyuruların yaygınlaştırılmasına karar verildi.
3. Öğretmenlerin müfredatlarına e-Güvenlik etkinliklerini entegre etmesine, güvenli internet gününde Eba siber güvenlik portalındaki kaynakların izlettirilmesine güvenli internet ve bilgisayar kullanımı hakkında bilgilendirme yapılmasına ve okul web sitesindeki dökümanların takip edilmesine karar verildi.
4. Rehber öğretmeni tarafından verilen e-bağımlılık, e-güvenlik , bilnçli internet kullanımı gibi eğitimlere katılım sağlanmasına ayrıca çevrimiçi eğitimlere de katılım sağlanmasına karar verildi.
5. Öğretmenlerimizin ve varsa cep telefonu kullanan öğrencilerimizin cep telefonlarını ders, toplantı ,tören vb etkinliklerde sessize almalarına ,telefon konuşmalarının etkinlik sonrasında yapılmasına karar verildi.Ayrıca sosyal medya genelgesinin okunarak genelgeye uygun hareket edilmesine karar verildi.
6. e-Güvenlik okul politikasının okul web sitesinde yayınlanmasına ve bütün öğretmenlerin okul politikasını okumalarına ve politikaya uygun hareket etmelerine karar verildi.
7. eTwinning projelerinde ve diğer etkinliklerde öğrenci resimlerinin kullanılması için velilerden onay alınmasına karar verildi.
8. Okulumuzda yürütülen eTwinning projelerine http://istiklalilkokulu.meb.k12.tr/ web adresinden ulaşılmasına ve yürütülen projelerin bütün öğretmenler tarafından incelenmesine karar verildi.
9. eTwinning okulu olmak için eTwinning çalışmalarına her türlü desteğin verilmesine karar verildi.
10. Toplantı iyi dilek ve temennilerle sona erdi.

Tuba Didem KARADOĞAN
Okul Öncesi Öğrt.

Gülsen KAMA
Okul Öncesi Öğrt.

Nezahat DEMİRCİ DURUK
İngilizce Öğrt.

Filiz ÖZKAN
Sınıf Öğrt.

Turgay IŞIK
Sınıf Öğrt.

Nagihan KALENDEROĞLU
Sınıf Öğrt.

Kadriye KAYA TUTAR
Sınıf Öğrt.

Güliz AFACAN
Sınıf Öğrt.

Zühre KANDEMİR EŞGÜNOĞLU
Sınıf Öğrt.

Fatma GÜLKAYA
Sınıf Öğrt.

Açelya YAMAN
Sınıf Öğrt.

Müjde ZENGİ
Sınıf Öğrt.

Tansel TÜRKMEN(Raporlu)
Sınıf Öğrt.

Zekeriya YALIM
Sınıf Öğrt.

Aynur YILMAZ ATLI
Sınıf Öğrt.

İlknur DEMİRTAŞ
Sınıf Öğrt.

Nursel TEKELİ
Sınıf Öğrt.

Rabia TUNCİL CAN
Sınıf Öğrt.

Sevinç BİLGİÇ
Sınıf Öğrt.

Demet TAŞDAN (Raporlu)
Rehber Öğrt.

Zafer EKİCİ
Görevlendirme
Sınıf Öğrt.

Nagihan AKÇA
Görevlendirme
Sınıf Öğrt.

Gökçe AYDIN
Görevlendirme
Sınıf Öğrt.

Bülent ÜNGÖR
Müdür Yard.

Mutlu GENÇ
Okul Müdürü

Okulumuz öğretmenleri ile birlikte okul politikası oluşturulmuştur. Bununla birlikte eSafety Label Bronz etiketi alınmıştır.
http://istiklalilkokulu.meb.k12.tr/icerikler/guvenli-internetesafety-label-bronz-etiketimizi-aldik_10611136.html
Okulumuzun giriş kısmında e-güvenlik panomuz vardır. Öğretmenler kurulu kararlarında e-güvenlik ile ilgili yapılacak çalışmalara yer verilmiştir. Öğrenci, öğretmen ve veliler düzenli olarak e-güvenlik eğitimi almışlardır. Öğrenci, öğretmen ve velilerimize,dijital bağımlılık , çevrimiçi güvenlik ,siber zorbalık ,internet güvenliği ve dijital ayak izi konusunda bilgilendirme etkinlikleri yapıldı. Bu kapsamda velilere, öğrencilere ve öğretmenlere WhatsApp üzerinden Özel Eğitim ve Rehberlik Hizmetleri Genel Müdürlüğünün bilgilendirme broşürleri paylaşıldı.
https://orgm.meb.gov.tr/meb_iys_dosyalar/2019_12/26113028_GUVENLY_YNTERNET_KULLANIMI.pdf
Projelerimizde veli izin belgesi alarak öğrencilerimizi projeye dahil ediyoruz. Okulumuz,internet güvenliğiyle ilgili anket yapıp sonuçlarını okul web sayfamızda paylaşmıştır.
http://istiklalilkokulu.meb.k12.tr/meb_iys_dosyalar/06/25/265074/dosyalar/2020_12/03112630_esafety_label_results.docx
11 Şubat 2020 ‘de Güvenli İnternet Günü kutlaması yapılmış ve yapılan çalışmalar okul panolarında sergilenmiştir. Okul politikamızda, okul stratejik planında ve swot analizinde e güvenlik ile ilgili detaylı açıklamalarda bulunulmuştur. Okulumuzda öğrencilerin ,okul personelinin ve velilerin fotoğraf çekmesi ve yayınlamalarının denetimi ile ilgili hususlar okul politikamızda açıkça belirtilmiştir.
https://cdnimage.eba.gov.tr/beta/978/4b7/f3a/c3e/c88/334/749

http://istiklalilkokulu.meb.k12.tr/meb_iys_dosyalar/06/25/265074/dosyalar/2020_11/24141623_E_GUVENLYK_POLYTYKAMIZ_HAKKINDA.docx?CHK=180137bb8fb6e8b262ae2e0041560881