Our school's e-Safety policy

ŞEHİT TEĞMEN SUBUTAY ALKAN ORTAOKULU GÜVENLİ İNTERNET OKUL POLİTİKASI

Okul Güvenlik Politikaları hızla gelişti, çünkü paydaşlar bugün internete okul binasından çok çeşitli şekillerde erişebilirler. Günlük yaşamımızın bir parçası olarak hepimiz teknolojilerle yaşıyoruz. Çocuklarımızın dijital teknolojilerle elde ettikleri fırsatları en iyi nasıl kullanacaklarını bildiklerinden emin olmak için, artık bunları nasıl kullanacaklarını bilmeli ve anlayabilmeliyiz. Bunun evde, okulda ya da arkadaşlarınızla ya da yalnız kaldığınız yerlerde mümkün olan en güvenli ortamda yapılmasını sağlamak dikkat etmemiz gereken açık ve özlü bir Okul Politikamız vardır.

GÜVENLİ İNTERNET KULLANIMI KURALLARI

Emniyet, okuldaki her öğretmenin sorumluluğunu alırken, Okulun Güvenli İnternet Politikasının uygulanması, incelenmesi ve uygulanmasından sorumlu tek bir lider kişiye sahip olması gerekir. Okulumuzun, Güvenli İnternet Koordinatörü Bilişim Teknolojileri Öğretmenimiz Betül ÇELEBİ UZGUR'dur. Okulun Güvenli İnternet Politikasının uygulanmasını ve izlenmesini denetleyecek ve yılda en az bir kere olmak üzere Güvenli İnternet Komitesine ve Müdüre rapor edecek ve bu bilgilerin kullanımındaki önemli yeni gelişmeler ışığında daha düzenli olacaktır.

Okulun Güvenli İnternet Politikası, kadro, öğrenci ve velilerin güvenliği ile okulun itibarını ve geleceği ile ilgili dijital gelişmelere ve yeni trendlere ayak uydurmalıdır.

Okula Güvenli İnternet Politikasında atıfta bulunulan yasalar, Politikanın neleri kapsadığına ilişkin brifingler sırasında, örneğin, uygun davranış, bilgi paylaşımı veya yasadışı imgeler gibi, diğerleri arasında atıf yapılmasına ihtiyaç duyulmaktadır.

Okulun Güvenli İnternet Politikası, öğrencilerin çevrimiçi teknolojilerin sağlıklı kullanılması konusundaki bilincini teşvik ederken, önemli Güvenli İnternet alanlarında sağlam ve tutarlı olmalıdır.

Okulun Güvenli İnternet Politikası, AUP ile ve okuldaki güvenlikle ilgili diğer politikalarla (örn. Çocukların korunması, anti-sosyal davranış veya zorbalığa karşı korunma) uyumlu olmalıdır.

Paydaş katılımı önemlidir. Politikanın oluşturulmasında tüm paydaşları dahil etmekteyiz: öğrenciler, personel, veliler ve daha geniş topluluk mensupları. Bu, tüm grupların politikanın belirli bölümleri üzerinde mülkiyet sahibi olmasını ve bu gruplara uyma olasılıklarının artmasını sağlamaya yardımcı olmaktadır.

Okulun Güvenli İnternet politikası, açık ve net bir şekilde ifade edilmektedir, teknik olmayan dilde anlaşılması kolay ve tüm personelin ve öğrencilerin onlardan neler beklendiğini bilmelerini sağlayan açık kurallar bulunmaktadır..

Amaçlar ve politika kapsamı

• Şehit Teğmen Subutay Alkan Ortaokulu, çevrimiçi güvenliğin (e-Güvenlik), bilgisayarlar, tabletler, cep telefonları veya oyun konsolları gibi teknolojiyi kullanırken, dijital dünyadaki çocukların ve yetişkinlerin

Hale EVRİ[illegible]DEMİR
Okul Müdürü

korunması için vazgeçilmez bir unsur olduğuna inanmaktadır.

• Şehit Teğmen Subutay Alkan Ortaokulu, internetin ve bilgi iletişim teknolojilerinin günlük yaşamın önemli bir parçası olduğuna inanır. Dolayısıyla, riskleri yönetmeleri ve bunlara tepki vermek için stratejiler geliştirmenin yollarını öğrenmeleri için çocuklar desteklenmelidir.

• Şehit Teğmen Subutay Alkan Ortaokulu, eğitim standartlarını yükseltmek, başarıyı teşvik etmek, personelin mesleki çalışmalarını desteklemek ve yönetim işlevlerini geliştirmek için toplumun kaliteli İnternet erişimi sunma yükümlülüğüne sahiptir.

• Şehit Teğmen Subutay Alkan Ortaokulu, tüm çocukların ve personelin çevrimiçi olarak potansiyel zararlardan korunmasını sağlamakla sorumludur.

• Bu politika, yöneticiler, öğretmenler, destek personeli, çocuklar ve ebeveynler için hazırlanmıştır.

• Bu politika, internet erişimi ve kişisel cihazlar da dahil olmak üzere bilgi iletişim cihazlarının kullanımı için geçerlidir; çocuklar, personel ya da diğer kişilere, çalıştıkları dizüstü bilgisayarlar, tabletler veya mobil cihazlar gibi uzaktan kullanım için okul tarafından verilen cihazlar için de geçerlidir.

Tüm çalışanların sorumlulukları şunlardır:

• Çevrimiçi güvenlik politikalarının geliştirilmesine katkıda bulunmak.

• Kabul Edilebilir Kullanım Politikalarını okumak ve onlara bağlı kalmak.

• Okul sistemlerinin ve verilerin güvenliğinden sorumlu olmak.

• Bir dizi farklı çevrimiçi güvenlik konusundaki farkındalığa sahip olmak ve onların bakımında çocuklarla nasıl ilişkili olabileceklerini bilmek.

• Yeni ve gelişmekte olan teknolojiler kullanıldığında iyi uygulamaları modellemek.

• Mümkün olduğunca müfredat ile çevrimiçi güvenlik eğitimini ilişkilendirmek.

• Okul koruma politikalarını ve prosedürlerini takip ederek endişe duyan bireyleri belirlenmek ve önlem alınmak.

• Olumlu öğrenme fırsatlarına vurgu yapmak.

• Bu alanda mesleki gelişim için kişisel sorumluluk almak.

Çocukların başlıca sorumlulukları şunlardır:

• Çevrimiçi güvenlik politikalarının geliştirilmesine katkıda bulunmak.

• Okulun Kabul Edilebilir Kullanım Politikalarını okumak ve onlara bağlı kalmak.

• 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.

• 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.

Ebeveynlerin başlıca sorumlulukları şunlardır:

• Okul Kabul Edilebilir Kullanım Politikalarını okumak, çocuklarını bu politikaya bağlı kalmaya teşvik etmek ve uygun olduğunca kendilerinin de bağlı kalmasını sağlamak.

• 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 ve ya 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.

Okul / web sitesinin yönetilmesi

• 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 ebeveynlerinin 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.

Okulda Fotoğraf - Video Çekme ve Yayınlama

Kendi çocuğunuzu bir konserde veya okulda oynarken görmek, ebeveynler için unutulmaz ve gurur verici bir andır ve birçoğunun bir kamerada yakalamak isteyeceği bir şeydir. Bugün bir cep telefonundan sosyal medya sitesine hızlı erişim sayesinde, okul liderleri ve diğer personelin velileri bilgilendirmesi ve iletişim kurması için bazı kurallar vardır.

Çevrimiçi görüntü ve videolar yayınlama

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.

Ebeveyn izin vermezse, bunun öğrencinin neden olabileceği muhtemel sıkıntıyı göz önüne alınarak kesinlikle çekim yapılmaz.

Okuldaki herkes fotoğrafların ve video içeriğini sosyal medyada paylaşmanın etkilerini bildiğinden ASLA tam adı, yaşı veya diğer kişisel bilgileri çocuğun web sitesinde bir fotoğraf ile birlikte yayınlanmaz.

- 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 velilerden remi yazılı izni alınacaktır.

Eğitim amaçlı resmi video konferans ve web kamerası kullanımı

- Okul, video konferansın çok çeşitli öğrenme avantajlarıyla zorlu bir faaliyet olduğunu kabul eder. Hazırlık ve değerlendirme, tüm faaliyet için gereklidir.
- Tüm video konferans ekipmanları, kullanılmadığında ve uygun olduğunda kapatılacaktır, otomatik cevaplamaya ayarlanmayacaktır.
- Harici IP adresleri diğer sitelere sunulmayacaktır.
- Video konferans iletişim detayları kamuoyuna açık olarak paylaşılmayacaktır.
- Video konferans ekipmanları güvenli bir şekilde tutulacak ve gerekirse kullanılmadığında kilitlenecektir.
- Okul video konferans ekipmanları izinsiz olarak okul binalarından çıkarılmayacaktır.
- Personel, dış video konferans fırsatlarının ve / veya araçlarının uygun bir şekilde değerlendirildiğinden emin olacak ve olaylara erişmek için kullanılan hesapların ve sistemlerin uygun bir şekilde güvenli ve gizli olmasını sağlayacaktır.

Kullanıcılar

- Öğrenciler, bir video konferans araması veya mesajı hazırlamadan veya cevaplamadan önce bir öğretmenin izin isteyecektir.
- Video konferans, öğrencilerin yaşı ve yeteneği için uygun bir şekilde denetlenecek.
- Velilerin rızası, çocuklar video konferans faaliyetlerine katılmadan önce alınacaktır.
- Video konferans, sağlam bir risk değerlendirmesini takiben, resmi ve onaylanmış iletişim kanalları vasıtasıyla gerçekleşecektir
- Sadece ana yöneticilere video konferans yönetim alanlarına veya uzaktan kumanda sayfalarına erişim hakkı verilecektir.
- Eğitimsel video konferans servisleri için özel oturum açma ve şifre bilgileri yalnızca personellere verilecek ve gizli tutulacak.

Okul Müdürü

İçerik

• Bir video konferans dersi kaydederken, tüm siteler ve katılımcılar tarafından yazılı izin alınacaktır. Konferansın başlangıcında kayıt nedeni belirtilmeli ve video konferans kaydı tüm taraflara açık olmalıdır. Kaydedilen malzemeler güvenli bir şekilde saklanacaktır.

• Üçüncü taraf materyalleri dahil edilecekse, okul üçüncü şahsın fikri mülkiyet haklarını ihlal etmekten kaçınmak için bu kaydın kabul edilebilir olup olmadığını kontrol edecektir.

• Okul, bir video konferansa katılmadan önce diğer konferans katılımcılarıyla diyalog kuracak. Okul değilse, okul sınıf için uygun olan materyali teslim aldığını kontrol edecektir.

İnternetin ve ilgili cihazların uygun ve güvenli kullanımı

• 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. Daha fazla bilgi için lütfen özel müfredat politikalarına erişin.

• Okulun internet erişimi eğitimi geliştirmek ve genişletmek için tasarlanacaktır.

• İnternet erişim seviyeleri müfredat gereklilikleri ve öğrencilerin yaş ve yeteneklerini yansıtacak şekilde gözden geçirilecektir.

•Çalışanların tüm üyeleri, çocukları korumak için tek başına filtrelemeye güvenmeyeceklerinin farkındadır ve gözetim, sınıf yönetimi ve güvenli ve sorumlu kullanım eğitimi önemlidir.

• Öğrencilerin yaşlarına ve yeteneklerine uygun olacaktır.

• Tüm okul ait cihazlar, okulun Kabul Edilebilir Kullanım Politikasına uygun olarak ve uygun güvenlik ve güvenlik önlemleri alınarak kullanılacaktır.

• Personel üyeleri, web sitelerini, araçlarını ve uygulamalarını sınıfta kullanmadan önce veya evde kullanmayı önerirken daima değerlendirecektir.

• Öğrenciler, bilginin konumlanması, alınması ve değerlendirilmesi becerileri de dahil olmak üzere, İnternette araştırmada etkili kullanımı konusunda eğitilecektir.

• Okul, personelin ve öğrencilerin İnternet'ten türetilen materyallerin telif hakkı yasalarına uygun olmasını ve bilgi kaynaklarını kabul etmesini sağlayacaktır.

• Öğrencilere, okudukları ve ya gösterilen bilgilerin doğruluğunu kabul etmeden önce eleştirel düşünmeleri öğretilecektir.

• Çevrimiçi materyallerin değerlendirilmesi, her konuda öğretme ve öğrenmenin bir parçasıdır ve müfredatta bir bütün olarak görülür.

• Okul, öğrencileri ve çalışanlarımızın güvenli ve gizli bir ortamda iletişim kurmalarını ve işbirliği yapmalarını sağlamak için interneti kullanacaklardır.

OKULLARDA CEP TELEFONLARINI KULLANMA

Cep telefonlarında mutlak [illegible]

Okul Müdürü

ebeveyn, çocuklarına daima erişebilmeleri konusunda ısrarcı davrandıkları için giderek zorlaşmaktadır. Cep telefonlarının varlığı yıkıcı olabilir ve aldatma ve zorbalık gibi yıkıcı davranışlara neden olsa da, bulundukları yer ve kullanım hakkında sıkı bir politika yürürlükte olduğu sürece, sınıfta proaktif ve yaratıcı bir şekilde kullanıldığında benzeri görülmemiş fırsatlar sunabilirler.

Kişisel Cihazların ve Cep Telefonlarının Kullanımı

• Cep telefonlarının ve çocukların, gençlerin ve yetişkinler arasındaki diğer kişisel cihazların yaygın bir şekilde sahiplenilmesi, tüm üyelerin Şehit Teğmen Subutay Alkan Ortaokulu topluluğunun cep telefonlarının ve kişisel cihazların sorumlu bir şekilde kullanılmasını sağlamak için gerekli adımları atmalarını gerektirir .

• Gençlerin ve yetişkinlerin cep telefonlarının ve diğer kişisel cihazların kullanımı, okul tarafından kararlaştırılacak ve okul Kabul Edilebilir Kullanım veya Cep Telefonu Politikası dahil olmak üzere uygun politikalarda yer alacaktır.

• Şehit Teğmen Subutay Alkan 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.

Kişisel cihazların ve cep telefonlarının güvenli bir şekilde kullanılması için beklentiler

• Kişisel cihazların ve cep telefonlarının kullanımı yasaya ve diğer uygun okul politikalarına uygun olarak yerine getirilecektir.

• Sahaya getirilen her türlü elektronik cihazın sorumluluğu kullanıcıya aittir. Okul, bu tür öğelerin kaybı, çalınması veya zarar görmesi konusunda sorumluluk kabul etmez. Okul, bu tür cihazların potansiyel veya fiili neden olduğu olumsuz sağlık etkileri için sorumluluk kabul etmez.

• Kötüye kullanım veya uygun olmayan mesajların veya içeriğin cep telefonları veya kişisel cihazlarla gönderilmesi, topluluğun herhangi bir üyesi tarafından yasaklanır ve herhangi bir ihlal, disiplin / davranış politikasının bir parçası olarak ele alınacaktır.

• Şehit Teğmen Subutay Alkan Ortaokulu topluluğunun tüm üyelerine cep telefonlarını veya cihazlarını kayıp, hırsızlık veya hasardan korumak için adım atmaları önerilir.

• Şehit Teğmen Subutay Alkan Ortaokulu topluluğunun tüm üyelerinden, kayboldukları veya çalındığı takdirde yetkisiz aramaların veya hareketlerin telefonlarında veya cihazlarında yapılamayacağından emin olmak için şifreler / pin numaraları kullanmaları önerilir. Parolalar ve pin numaraları gizli tutulmalıdır. Cep telefonları ve kişisel cihazlar paylaşılmamalıdır.

• Şehit Teğmen Subutay Alkan Ortaokulu topluluğunun tüm üyelerine, cep telefonlarının ve kişisel cihazlarının saldırgan, küçümseyen veya başka şekilde okul / ayar politikalarına aykırı düşen herhangi bir içerik içermediğinden emin olmaları önerilir.

Öğrencilerin kişisel cihazlar ve cep telefonları kullanımı

• Öğrenciler, kişisel cihazların ve cep telefonlarının güvenli ve uygun kullanımı konusunda eğitim alacaklardır.

• Çocukların cep telefonlarının ve kişisel cihazların tüm kullanımları yaşlarına uygun olarak kısıtlanacaktır.

Hale EVİRGEN DEMİR
Okul Müdürü

• Cep telefonları veya kişisel cihazlar, öğrencilerin bir öğretim üyesinin onayını alarak onaylanmış ve yönlendirilmiş müfredat tabanlı etkinlik kapsamında olmadıkları sürece dersler veya resmi okul saatlerinde öğrenciler tarafından okula getirilemez.

• 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.

• Öğrenciler, telefon numaralarını yalnızca güvenilir arkadaşlarına ve aile üyelerine vermelidirler.

• Öğrencilere, cep telefonlarının ve kişisel cihazların güvenli ve uygun bir şekilde kullanımı öğretilecek ve sınırların ve sonuçların farkına varılacaktır.

•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.

Personelin kişisel cihazlar ve cep telefonları kullanımı

• Personelin, kendi kişisel telefonlarını veya cihazlarını, çocukların, gençlerin ve ailelerinin, mesleki bir kapasitede, ortamın içinde veya dışındaki bölgeleriyle bağlantı kurmalarına izin verilmez. Bu konuyu tehlikeye atacak önceden var olan ilişkiler yöneticilerle görüşülecektir.

• Personel, çocukların fotoğraflarını veya videolarını çekmek için cep telefonları, tabletler veya kameralar gibi kişisel cihazları kullanmaz ve yalnızca bu amaçla işle sağlanan ekipmanı kullanır.

• Personel herhangi bir kişisel cihazı doğrudan çocuklarla kullanmaz ve ders / eğitim etkinlikleri sırasında yalnızca okul tarafından sağlanan ekipmanı kullanır.

• Personel, kişisel telefonların ve cihazların herhangi bir şekilde kullanımının daima veri koruma ve ilgili okul politikası ve prosedürleri uyarınca yerine getirilmesini sağlayacaktır.• Personel kişisel cep telefonları ve cihazları ders saatlerinde kapatılıp / sessiz moda geçirilir.

• Bluetooth veya diğer iletişim biçimleri ders saatlerinde *"gizlenmiş"* veya kapalı olmalıdır.

• Acil durumlarda okul idaresi tarafından izin verilmemişse, kişisel cep telefonları veya cihazları öğretim dönemleri boyunca kullanılamaz.

• Personel, cep telefonları ve kişisel cihazlar üzerinden sitede satın alınan içeriğin profesyonel rolü ve beklentileri ile uyumlu olmasını sağlayacaktır.

• Bir personel okul politikasını ihlal ettiği durumlarda disiplin işlemi yapılır.

• Bir personelin, bir cep telefonuna veya kişisel bir cihaza kaydedilen veya saklanan yasadışı içeriğe sahip olduğu veya ceza gerektiren bir suç işlemiş olması durumunda, polise ulaşılacaktır.

• Personelin cep telefonunu veya cihazlarını kişisel olarak kullanmalarını içeren herhangi bir iddiaya okul yönetim politikasını izleyerek yanıt verilecektir.

Çocukların eğitimi

• Öğrenciler arasında güvenli ve sorumlu internet kullanımının önemi ile ilgili farkındalık yaratmak için bir çevrimiçi güvenlik (e-Güvenlik) müfredatı oluşturulur ve okulun tamamında yer alır.

• Güvenli ve sorumlu kullanım ile ilgili eğitim internet erişiminden önce yapılacaktır.

Okul Müdürü

• Müfredat geliştirme ve uygulama da dahil olmak üzere okul çevrimiçi güvenlik politikaları ve uygulamaları yazarken ve geliştirirken öğrenci katkıları aranacaktır.

• Öğrenciler, Kabul Edilebilir Kullanım Politikasını, yaşlarına ve yeteneklerine uygun bir şekilde okumak ve anlamak için desteklenecektir.

• Tüm kullanıcılara ağ ve internet kullanımının izleneceği bildirilecektir.

• Kabul Edilebilir Kullanım beklentileri ve Posterler, Internet erişimi olan tüm odalarda yayınlanacaktır.

• İnternetin ve teknolojinin güvenli ve sorumlu kullanımı, müfredatta ve tüm konularda güçlenecektir.

• Dışarıdan destek, okulların dahili çevrimiçi güvenlik (e-Güvenlik) eğitim yaklaşımlarını tamamlamak ve desteklemek için kullanılacaktır.

• Okul, öğrencilerin teknolojiyi olumlu şekilde kullandıklarını ödüllendirecektir.

• Okul, öğrencilerin ihtiyaçlarına uygun olarak çevrimiçi güvenliği geliştirmek için akran eğitimini uygulayacaktır.

• Okulda daha güvenli internet gününün (SID) kutlanacak ve yapılacak etkinliklerle güvenli internet hakkında bilgi verilecektir.

Personelin eğitimi

• 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 tüm üyeleri, çevrimiçi davranışlarının okuldaki rolü ve itibarını etkileyebileceğinin farkına varacaktır. Mesleği veya kurumu çürüme durumuna düşürdüğü veya profesyonel yeteneklerine güvenini kaybetmiş bir şeyin bulunduğu düşünülürse, kamusal, disiplin veya hukuki önlemler alınabilir.

• Filtreleme sistemlerini yönetme veya BİT kullanımını izleme sorumluluğu taşıyan personelin üyeleri, Liderlik Ekibi tarafından denetlenecek ve sorunları veya endişeleri bildirmek için açık prosedürlere sahip olacaklar.

• Okul, çalışanların öğrencilerin yaşlarına ve yeteneklerine göre kullanması gereken yararlı çevrimiçi araçları vurgulamaktadır.

Ebeveynlerin eğitimi

• Şehit Teğmen Subutay Alkan Ortaokulu, çocukların internetin ve dijital teknolojinin güvenilir ve sorumlu kullanıcıları olabilmesi için ana-babaların oynayacakları önemli bir role sahip olduklarını kabul eder.

• Ebeveynlerin dikkatleri, okul açıklamaları ve okul web sitesinde okul çevrimiçi güvenlik (e-Güvenlik) politikasına ve beklentilerine yönelecektir.

• Okul Anlaşması'nın bir parçası olarak ebeveynlerin çevrimiçi güvenlik bilgilerini okumaları istenecektir.

• Ebeveynler, Okula Kabul Edilebilir Kullanım Politikası'nı okumaya ve çocuklarının etkileri[illegible] tartışmaya

teşvik edilecektir.

• Çevrimiçi güvenlik konusundaki ebeveynler için bilgi ve rehberlik, ebeveynlere çeşitli biçimlerde sunulacaktır.

• Ebeveynlerin, çevrimiçi olarak çocukları için olumlu davranışları rol modellemeleri teşvik edilecektir.

Çevrimiçi Olaylara ve Koruma sorunlarına yanıt verme

• Okulun tüm üyeleri, çevrimiçi / siber zorbalık vb. dahil olmak üzere karşılaşılabilecek çevrimiçi risklerin çeşitliliğinden haberdar edilecektir. Bu, öğrencilere yönelik personel eğitimi ve eğitim yaklaşımları içerisinde vurgulanacaktır.

• Okulun tüm üyeleri, filtreleme, siber zorbalık, yasadışı içerik ihlali vb. gibi çevrimiçi güvenlik (e-Güvenlik) endişelerini bildirme prosedürü hakkında bilgilendirilecektir.

• Dijital Abone Hattı (DSL), daha sonra kaydedilecek olan çocuk koruma endişelerini içeren herhangi bir çevrimiçi güvenlik (e-Güvenlik) olayı hakkında bilgilendirilecektir.

• İnternet'in yanlış kullanımı ile ilgili şikayetler, okulun şikayet prosedürleri kapsamında ele alınacaktır.

• Çevrimiçi / siber zorbalık ile ilgili şikayetler, okulun zorbalık karşıtı politikası ve prosedürü kapsamında ele alınacak

• Personelin yanlış kullanımı ile ilgili herhangi bir şikayet okul müdürüne yönlendirilecektir

• Okul şikayet prosedürü öğrencilere, velilere ve personele bildirilecektir.

• Şikayet ve ihbar prosedürü personele bildirilecektir.

• Okulun tüm üyeleri, gizliliğin öneminden ve endişeleri bildirmek için resmi okul usullerine uyma ihtiyacından haberdar olmalıdırlar.

• Okulun tüm üyeleri, çevrimiçi ortamda güvenli ve uygun davranış hakkında hatırlatılacak ve okul camiasının herhangi bir diğer üyesine zarar vermek, sıkıntı yaşamak veya suç oluşturan herhangi bir içerik, yorum, resim veya video yayımlamamanın önemini hatırlatacaktır.

• Okul, çevrimiçi güvenlik (e-Güvenlik) olaylarını, uygun olduğunda, okul disiplini / davranış politikasına uygun olarak yönetir.

• Okul, ebeveynlere, ihtiyaç duyulduğunda bunlarla ilgili endişeleri bildirir.

• Herhangi bir soruşturma tamamlandıktan sonra okul bilgi alacak, öğrenilen dersleri belirleyecek ve değişiklikleri gerektiği gibi uygulayacaktır.

• Sorunları çözmek için ebeveynlerin ve çocukların okulla ortak çalışması gerekir.

İlde [illegible]
Okul Müdürü

Ailemizin Güvenli İnternet Sözleşmesi

.....Öğrenci..... Sözü

- Ailemin ve kendimin kişisel bilgilerini kimse ile paylaşmayacağım.
- Bilgisayarıma virüs, solucan gibi zararlı programların bulaşmasına neden olacak aktivitelerde bulunmayacağım.
- Tehlikelerden uzak kalabilmek için İnternet'te neler yaptığımı her zaman aileme söyleyeceğim.
- İyi bir oyuncu olacağım, kimsenin beni kandırmasına izin vermeyeceğim.
- Tanımadıklarımla sohbet etmeyeceğim, buluşmayacağım.
- Paylaşımda bulunurken dikkatli olacağım. Dosya ve müzik indirmeden önce anne ve babama danışacağım.
- İnternet şifrelerimi ailemden başka kimseye vermeyeceğim.
- Tanımadığım kimselerden gelen e-posta veya mesajlara cevap vermeyeceğim.
- Kurallara uyacağım ve "Akıllı Kullanıcı" olacağım.
- İnternet ve bilgisayar başında kalacağım zamanı iyi ayarlayacağım.
- Bedenimi koruyarak sağlıklı kalacağım.

Giray Çağlar ŞAHİN

İmza .....

.....Veli..... Sözü

- Çocuğumla, İnternet kullanırken başına gelebilecek her türlü durum hakkında konuşup bilgilenmesini sağlayacağım.
- Uygun olmayan İnternet içeriklerinden çocuğumu korumak için filtreleme ve güvenlik programları kullanacağım.
- Çocuğum İnternet'te karşılaştığı kötü bir durumu bana anlattığı zaman aşırı tepki göstermeyeceğim.
- Bilgisayar ve İnternet kullanımı konusunda mantıklı ve kabul edilebilir kurallar koyacağım.
- Çocuğumun çevrimiçi arkadaş listesi ve arkadaş iletişim bilgileri hakkında bilgi sahibi olacağım.
- Çocuğum için tavsiye edilebilir güvenli İnternet siteleri bulacağım.
- Çocuğumun İnternet'i ve bilgisayarı daha güvenli kullanmasını sağlayacağım.
- Güvenli kullanıcı olması için onu hep destekleyeceğim.
- Lisanslı programlar kullanarak, başkalarının telif haklarına saygılı davranarak çocuğuma örnek olacağım.
- Onun İnternet dışında başka aktivitelere katılmasına destek olacağım.
- Bilgisayarı ev içerisinde ortak bir alana yerleştireceğim. Uygun masa ve sandalye kullandıracağım.

Fikz ŞAHİN

İmza .....

Hale EVRİ
Okul Müdürü

We use this file to taking permission from our students and parents about esafety policy.

Sevgili Öğrencimiz ve Sayın Velimiz,

İnternet, bilgisayarların küresel ağa bağlanmasıyla dünya üzerindeki var olan bilginin değerlendirilmesi ve erişilmesine olanak tanımaktadır. Bu durum öğrencilere; fikir zenginliği,bilgi alışverişi, dünya üzerindeki farklı ülkelerden organizasyonlarda profesyonel insanlarla iletişim kurma fırsatı sağlar. Güvenli ve sorumlu internet kullanan dijital bireyler yetiştirirken anne babalardan desteklerine ihtiyaç duyduğumuz konuları aşağıda belirttik. Katkılarınız için teşekkür ederiz.

Saygılarımızla
Okul Yönetimi

İNTERNET POLİTİKAMIZ

Şehit Teğmen Subutay Alkan Ortaokulu'nda öğrencilere, bilişim teknolojileri dersliklerinde, elektronik sınıflarda, öğrenme faaliyetlerinin bir parçası olarak internet kaynaklarına erişim imkanı verilmektedir. İnternet üzerindeki tüm bilgilerin kontrol edilmesi ve düzenlenmesi okulumuz tarafından teknik olarak mümkün değildir. Bu nedenle önlem olarak, okulumuzda bilgisayar dersliklerinde, ekran kontrol programları kullanılmakta, bu programlar aracılığı ile öğrenci ekranlarının internet kontrolü ve genel çalışmalara yönelik yönlendirmeleri yapılmaktadır. Böylece istenmeyen internet sitelerine girişler önlenebilmektedir. Bilişim Teknolojileri bölümü öğretmenleri ve diğer öğretmenlerimiz, öğrencilerimizin internet kullanırken kabul edilebilir sorumluluklar içinde her kullanıcının davranışının ve sorumluluğunun kendilerine ait olduğuna dair bir bilinç geliştirmelerine yardımcı olmaya devam etmektedirler. Okul içinde bu sorumluluk tamamen öğrenciye aittir. Eğer öğrenciler okul dışında, kasıtlı olarak istenmeyen / yasal olmayan siteleri kullanırlarsa, bilgi paylaşırlarsa, bu durum tamamen öğrenci ve dolayısıyla velinin sorumluluğundadır.

Okulumuz bilgisayarları ve internet erişimi öğrenmeye yardımcı olmak amaçlıdır. İnternetin güvenli kullanılması okuldaki herkese katkı sağlayacağı için aşağıdaki kurallar ortak faydada uygulamaya konulmuştur.

Öğrencilerimiz için Güvenli internet kullanım kuralları ve sorumlulukları:

- ✓ İnternet üzerinde başka kişilerin kişisel bilgilerini ve şifrelerini kullanmayacağım.
- ✓ Sadece uygun olan, kullanım hakkı verilen ve ihtiyaç duyulan eğitim materyallerine erişeceğim ve kayıt edeceğim.
- ✓ Yasal olmayan ve/veya Bilişim Teknolojileri Birimi tarafından izin verilmeyen siteleri (Ahlaki değerler taşımayan, şiddet içerikli internet siteleri sohbet programları gibi) kullanmayacağım.
- ✓ Sitelere kayıt olurken yaş sınırına dikkat edeceğim.
- ✓ Kişisel bilgilerimi (Ev adres bilgileri, telefon, kimlik bilgileri, resim, video gibi) internet üzerinde yayınlamayacağım.
- ✓ İnternetin özgür dünyasında diğer kullanıcıların söz ve davranışlarına, kültürel özelliklerine ve ana dillerine saygı duyacağım ve nazik olacağım.
- ✓ İnternet kullanırken okul işlerimi ve sorumluluklarımı önceliğime alacağım.
- ✓ İnternet aracılığıyla kasıtlı olarak başkalarına zarar verme amaçlı yapılan sanal zorbalığı uygulamayacağım.
- ✓ İnternet kullanırken eğer bana kötü davranılıyor, uygun olmayan mesajlar gönderiliyor, benim itibarıma ve arkadaşlıklarıma zarar veriliyorsa bunu ailemle veya öğretmenlerimle paylaşacağım.

İnternet Kullanım Etiğinin İmzalanması

Belirtilen kurallara uygun davranış göstermeyen öğrenciler okul içindeki internet kullanım haklarını kaybederler. İhtiyaç duyulan durumlarda öğrenci internet kullanımında kabul edilemez davranışı nedeniyle, Öğrenci Davranışlarını Değerlendirme Kurulu'na sevk edilir.

Tüm bu olasılıkları göz önüne alarak internet kullanımı hakkında yazılan bilgileri ve kuralları okudum, sorumluluklarımı ve kurallara uymadığımda sonuçlarını kabul ediyorum.

Tarih: 21/09/2020

Öğrencinin Adı Soyadı: Giray Gaglar ŞAHİN ..... Sınıfı: 6/B ... Öğrenci İmzası: .....

Çocuğumun velisi olarak yukarıda paylaşılan güvenli ve sorumlu internet kullanımı kurallarıyla ilgili sorumluluğu kabul ediyorum.

Velinin Adı Soyadı : Filiz ŞAHİN ..... İmzası: .....

Hale EVİRGEN DEMİRAN
Okul Müdürü

We use this file to taking permission from our students and parents about esafety policy.

ŞEHİT TEĞMEN SUBUTAY ALKAN ORTAOKULU MÜDÜRLÜĞÜ
ÖĞRENCİ SOSYAL MEDYA VELİ İZİN BELGESİ

Milli Eğitim Bakanlığımız 2017/12 Sayılı Genelgesi uyarınca, okulumuz....6-B.... sınıfında eğitim görmekte olan , velisi bulunduğum .....Gülay Doğan ŞAHİN isimli öğrencinin eğitim öğretim faaliyetleri kapsamında alınan ses, görüntü ve video kayıtlarının aynı zamanda hazırlamış olduğu eserlerin (hikaye, resim, fotoğraf, şiir, vb.) Milli Eğitim Bakanlığı'na bağlı kurum ve kuruluşlarca kullanılan kurumsal internet siteleri ve sosyal medya hesaplarında yayınlanmasına izin veriyorum / vermiyorum.

Gereğini arz ederim.

☒ İzin veriyorum.
☐ İzin vermiyorum.

Tarih : 21/09/2020

Veli İmzası :

Velinin Adı ve Soyadı : Filiz ŞAHİN

Hale EVİRCAN DEMİR
Okul Müdürü

ŞEHİT TEĞMEN SUBUTAY ALKAN ORTAOKULU

2020-2021 DERS YILI 5.SINIF BİLİŞİM TEKNOLOJİLERİ DERSİ ÜNİTELENDİRİLMİŞ YILLIK PLANI

This document is about integrating the safe use of the internet into the curriculum

Class 5

AY	HAFTA	SAAT	KAZANIMLAR	KONULAR	YÖNTEM VE TEKNİKLER	ARAÇ GEREÇ VE MATERYALLER	ATATÜRKÇÜLÜK / BELİRLİ GÜN VE HAFTALAR	ÖLÇME VE DEĞERLENDİRME
	[illegible]	2	[illegible]	BT.5.1.2. Araştırma	Anlatım, soru-cevap, tartışma	Akıllı Tahta, "İnternet Kullanım Grafiği" Afişi, "İnternetin Yararları Öğreniyorum" Sunumu	Dünya Çocuk Hakları Günü (20 Kasım) 24 Kasım Öğretmenler Günü	
	[illegible]	2	[illegible]	BT.5.1.2. Araştırma	Anlatım, soru-cevap, tartışma	"İnternet" Afişi, Web Değerlendirme Formu, Web Değerlendirme Afişi, EBA Güvenli Kullanım Kılavuzu	Dünya Engelliler Günü (3 Aralık)	
	[illegible]	2	[illegible]	BT.5.1.3. İletişim Teknolojileri ve İş Birliği	Anlatım, soru-cevap, tartışma, uygulama	Akıllı Tahta, İletişim Araçları Tanıtım Kağıtları	İnsan Hakları ve Demokrasi Haftası (10 Aralık)	
4. ÜNİTE: BT.5.4. ÜRÜN OLUŞTURMA								
ARALIK	[illegible]	2	[illegible]	BT.5.4.1. Görsel İşleme Programları	Anlatım, soru-cevap, tartışma, uygulama	Akıllı Tahta, Bilgisayar, "Çizim mi yoksa Fotoğraf mı?" Sunumu, "Görsel İşleme Programları" Afişi		
	[illegible]	2	[illegible]	BT.5.4.2. Kelime İşlemci Programları	Anlatım, soru-cevap, tartışma, uygulama	Akıllı Tahta, Bilgisayar, "Kelime İşlemci Programları" Sunumu, "Google Dokümanlar" Sunumu, "LibreOffice'i Tanıyalım" Görseli		
	[illegible]	2	[illegible]	BT.5.4.2. Kelime İşlemci Programları	Anlatım, soru-cevap, tartışma, uygulama	Akıllı Tahta, Bilgisayar, Kelime İşlemci Programı		
	[illegible]	2	[illegible]	BT.5.4.2. Kelime İşlemci Programları	Anlatım, soru-cevap, tartışma, uygulama	Akıllı Tahta, Bilgisayar, Kelime İşlemci Programı		2. SINAV
OCAK	[illegible]	2	[illegible]	BT.5.4.3. Sunu Programları	Anlatım, soru-cevap, tartışma, uygulama	Akıllı Tahta, Bilgisayar, Sunum Programı	Enerji Tasarrufu Haftası	
	[illegible]	2	[illegible]	BT.5.4.3. Sunu Programları	Anlatım, soru-cevap, tartışma, uygulama	Akıllı Tahta, Bilgisayar, Sunum Programı		
YARI YIL TATİLİ								
5. ÜNİTE: BT.5.5. PROBLEM ÇÖZME VE PROGRAMLAMA					KAZANIMLAR			
AY	HAFTA	SAAT	KAZANIMLAR	KONULAR	YÖNTEM VE TEKNİKLER	ARAÇ GEREÇ VE MATERYALLER	ATATÜRKÇÜLÜK / BELİRLİ GÜN VE HAFTALAR	ÖLÇME VE DEĞERLENDİRME
	[illegible]	2	BT.5.5.1.1. Problem çözmede temel kavramları tanımlayarak problem türlerini açıklar. BT.5.5.1.4. Problem çözme sürecinde takip edilmesi gereken adımları fark eder. BT.5.5.1.5. Verilen bir problemi analiz eder. BT.5.5.1.7. Matematik ve bilgisayar bilimi arasındaki ilişkiyi tespit eder.	BT.5.5.1. Problem Çözme Kavramları ve Yaklaşımları	Anlatım, soru-cevap, tartışma, uygulama	Akıllı Tahta, Kart Kazı Oyunu Problemi, Hanoi Kuleleri Bilmecesi		
ŞUBAT	[illegible]	2	BT.5.5.1.1. Günlük hayatta karşılaşılan problemleri çözüm önerileri getirir. BT.5.5.1.2. Verilen bir problemin uygun adımları kullanarak çözer. BT.5.5.1.3. Problem çözmede temel kavramları tanımlayarak problem türlerini açıklar. BT.5.5.1.4. Problem çözme sürecinde takip edilmesi gereken adımları fark eder. BT.5.5.1.5. Verilen bir problemi analiz eder.	BT.5.5.1. Problem Çözme Kavramları ve Yaklaşımları	Anlatım, soru-cevap, tartışma, uygulama	Akıllı Tahta, Bir Kılıç Çalışma Kağıdı ile Bulut Kavramsal Etkinliği	Güvenli İnternet Günü kapsamında bu konu işlenecektir. As part of the safe internet day, awareness will be raised among students regarding the safe use of the internet. In this context, various awareness activities will be organized with students.	

2020 – 2021 DERS YILI ŞEHİT TEĞMEN SUBUTAY ALKAN ORTAOKULU
8. SINIF MATEMATİK DERSİ ÜNİTELENDİRİLMİŞ YILLIK DERS PLANI

This document is about integrating the safe use of the internet into the curriculum.Class 8

OCAK	16.HAFTA(11-17)	5 SAAT	M.8.2. CEBİR	M.8.2.1. Cebirsel İfadeler ve Özdeşlikler	M.8.2.1.3. Özdeşlikleri modellerle açıklar.	a) $(a \pm b)^2 = a^2 \pm 2ab + b^2$ ve $a^2 - b^2 = (a-b)(a+b)$ özdeşlikleriyle sınırlı kalınır. b) Özdeşliklerdeki katsayılar tam sayılardan seçilir.	
OCAK	17.HAFTA(18-24)	5 SAAT	M.8.2. CEBİR	M.8.2.1. Cebirsel İfadeler ve Özdeşlikler	M.8.2.1.4. Cebirsel ifadeleri çarpanlara ayırır.		
ŞUBAT	18.HAFTA(08-14)	5 SAAT	M.8.2. CEBİR	M.8.2.1. Cebirsel İfadeler ve Özdeşlikler	M.8.2.1.4. Cebirsel ifadeleri çarpanlara ayırır.	a) Ortak çarpan parantezine alma ile iki kare farkı ve $a^2 \pm 2ab + b^2$ biçimindeki tam kare ifadelerin çarpanlara ayırma işlemleri ele alınır. b) Cebirsel ifadelerdeki katsayılar ve kökleri tam sayılar içinde kalacak biçimde seçilir. c) Gruplandırarak çarpanlarına ayırma yöntemine girilmez. ç) Tam kare olmayan ikinci dereceden ifadelerin çarpanlara ayrılma işlemlerine girilmez.	**NOT: Güvenli internet günü kapsamında bu konu işlenecektir.** As part of the safe internet day, awareness will be raised among students regarding the safe use of the internet. In this context, various awareness activities will be organized with students.

Hale [illegible]
Okul Müdürü

2020-2021 EĞİTİM ÖĞRETİM YILI ŞEHİT TEĞMEN SUBUTAY ALKAN ORTAOKULU
1.DÖNEM MATEMATİK DERSİ ZÜMRE ÖĞRETMENLERİ TOPLANTI TUTANAĞIDIR.

This document is about integrating the safe use of the internet into the math council meeting.

Toplantı No	1
Toplantının Öğretim Yılı	2020 – 2021
Toplantının Dönemi	1. Dönem
Toplantının Tarihi ve yeri	26/08/2020 Saat: 12.30 - Öğretmenler Odası
Toplantıya Katılanlar	Mehmet TAVZAR (Müdür Yardımcısı),Ebru AKGÜN, Erol KESKİN, Sevilay DİNÇ, Nazlı MERMER YILMAZ, Özlem DİZİLİ DEMİRCİ

GÜNDEM MADDELERİ:

1) Açılış,yoklama ve yazman seçimi.
2) 1739 Sayılı Milli Eğitim Temel Kanunun Okunması.
3) 2019 – 2020 eğitim yılının 2. Dönem uzaktan eğitim faaliyetlerinin değerlendirilmesi ve eksiklerin giderilmesi
4) 2020 – 2021 eğitim yılında salgın nedeniyle uzaktan eğitim ve normalleşme sürecinde yapılacak çalışmaların planlanması değerlendirilmesi
5) Pandemi dönemi psiko-sosyal destek çalışmaları
6) Yıllık planların hazırlanması. Öğretim programlarının incelenerek programların çevre özellikleri de dikkate alınarak amacına ve içeriğine uygun olarak uygulanması
7) Matematik Eğitiminin Genel amaçları. Matematik öğretim programının genel amaçları.
8) Ders araç ve gereçlerinin kullanılması.(Materyal hazırlanması ve kullanılması.)
9) Öğrencinin derse hazırlığının kontrol edilmesi.
10) Matematik dersinin diğer dersler ile ilişkisi(Zümre öğretmenleri ile ilişkisi)
11) Öğretim yöntem ve tekniklerinin belirlenmesi.
12) Proje görevi konularının tespit edilmesi ve Proje görevi değerlendirilmesi.
13) Yazılı, ders içi performanslarda birlik ve beraberliğin sağlanması.
14) Özel eğitim ihtiyacı olan öğrenciler için bireyselleştirilmiş eğitim programları (BEP) ile ders planlarının görüşülmesi.
15) Matematik dersinin Atatürk İlke ve İnkılapları doğrultusunda işlenmesi.
16) Matematik dersinde başarıyı arttırmada alınabilecek tedbirler.
17) İş sağlığı ve güvenliği tedbirlerinin değerlendirilmesi
18) Güvenli İnternet Günü ve İnternetin güvenli kullanımı ile ilgili yapılacak çalışmalar.
19) Dilek ve temenniler.

Safe Internet Day and studies on the safe use of the internet.

Halis EVİK
Okul Müdürü

This document is about integrating the safe internet topic into the teachers' board meeting.

ŞEHİT TEĞMEN SUBUTAY ALKAN ORTAOKULU
2020-2021 DERS YILI
1. DÖNEM ÖĞRETMENLER KURULU TOPLANTISI
GÜNDEM MADDELERİ

1- Açılış ve Yoklama.
2- Saygı Duruşu ve İstiklal Marşı'nın Okunması.
3- Yazman Seçimi.
4- Okul Müdürünün Açılış Konuşması.
5- 2020-2021 Ders Yılı sene başı mesleki çalışma programı hakkında bilgilendirme.
6- Sınıf/Şube rehber öğretmenlerinin belirlenmesi.
7- 2020-2021 Ders Yılı Covid-19 Salgını koruma ve önleme tedbirleri kapsamında okul ortamında alınacak tedbirler ve uyulması gereken kurallar:
   a- Eğitim Kurumlarında Hijyen Şartlarının Geliştirilmesi ve Enfeksiyon Önleme Kontrol Kılavuzu.
   b- Covid-19 Salgın Yönetimi ve Çalışma Rehberi.
   c- Öğretmen Bilgilendirme Rehberi.
8- "Okulum Temiz" Belgelendirme Programı hakkında bilgilendirme.
9- 2020-2021 Ders Yılı Covid-19 Salgını sürecinde öğrencilerin öğrenme kazanımlarına ilişkin eksiklere yönelik planlanan "Tamamlayıcı Eğitim Programı" uygulama süreçleri hakkında bilgilendirme yapılması
10- Zümre başkanlarının seçimi, Zümre Öğretmenler Kurulu ve Zümre Başkanları Kurulu toplantısında gereken hususların görüşülmesi, toplantı tutanaklarının okul idaresine teslim tarihinin belirlenmesi.
11- Okul politikası, e - güvenlik uygulamaları ve eTwinning Projesi konularının görüşülmesi.
12- Dilek ve temenniler.
13- Kapanış.

Discussion of school policy, esafety practices and eTwinning project issues

Include school eSafety policy and eTwinning work in the school strategy plan

ŞEHİT TEĞMEN SUBUTAY ALKAN ORTAOKULU
2020-2024 STRATEJİK PLANI

Review of school eSafety Policy. Okul e-Güvenlik Politikasının gözden geçirilerek stratejik plan içerisine dahil edilmiştir .İlerideki yıllarda politikamızın düzenli bir şekilde oluşan ilerlemelere paralel olarak revize edilmesi planlanmaktadır.

e-Safety issues referred to in school policies (e.g. behaviour, anti-bullying, child protection. Okul politikalarında e-Güvenlik ile ilgili konular işlenmektedir.Değişen teknolojik çağa ayak uydurulması ve gelişmelerin daha rahat takip edilmesi gerekmektedir.Bu yüzden stratejik plan içerisinde e-güvenlik konularının daha geniş kapsamlı işlenmesi hedeflenmektedir.

The school has a policy on the use of mobile devices/mobile phones. Okulumuzda taşınabilir cihazların ,cep telefonlarının kullanımı hakkında politika kriterlerinin gözden geçirilmiş ve okul stratejik plan içerisine dahil edilmiştir.Bu konuyla ilgili olarak velilerimize ,öğrencilerimize ve öğretmenlerimize her geçen yıl daha detaylı bilgiler verilmesi ve belirlenen kurallar ölçüsünde bu hedeflerin gerçekleştirilmesi hedeflenmektedir.

Our school policy contains a section on the taking and publishing of photographs of, and by,pupils, parents and staff.Okul politikalarımız ;öğrencilerimizin ,velilerimizin ve okul personelinin fotoğraflarının çekilmesi ve onların okulda fotoğraf çekmesi ve yayınlaması konusunu da okul stratejik plan içerisine alarak bu konunun e-Güvenlik açısından fazlasıyla önemli olduğunun bilincinde olduğunu kanıtlamıştır.

eSafety is taught as part of the curriculum.e-Güvenlik konularının müfredatın bir parçası haline getirilmesi. Okul politikalarında e-Güvenlik ile ilgili konular işlenmektedir.

Our school provides eSafety information for parents.Okulumuzda velilere e-Güvenlikle ilgili bilgilendirme çalışmalarının yapılması.Yenilenen ve gelişen bilişim teknoloji çağında öğrencilerimizi ve velilerimizin gerçekleşen yeniliklerden tam olarak doğru bilgilere ulaşması konusunda düzenli olarak bilgilendirme çalışmalar hedeflenmekte ve bu konu stratejik plan dahiline alınmıştır.

All our staff receives regular training on eSafety issues.Okul personelinin e-Güvenlikle ilgili düzenli eğitim alması. Değişen teknolojik çağa ayak uydurulması ve gelişmelerin daha rahat takip edilmesi gerekliliği esastır.Bu yüzden stratejik plan içerisinde bu bahsi geçen konuların daha geniş kapsamlı işlenmesi ve ele alınması hedef haline getirilmektedir.Öğretmenlerimizin gerekli eğitimleri düzenli bir şekilde alması planlanmaktadır.

Celebrating 'Safer Internet Day' (SID) in our school .Okulumuzda 'Daha Güvenli İnternet Günü (SID) 'nün düzenli bir şekilde kutlanması stratejik plan içerisine dahil edilmektedir.

Dissemination and development of eTwinning project work. eTwinning proje çalışmalarının yaygınlaştırma çalışmaları hedeflenmektedir.

GÜVENLİ İNTERNET GÜNÜ ÖĞRENCİ ETKİNLİKLERİMİZ

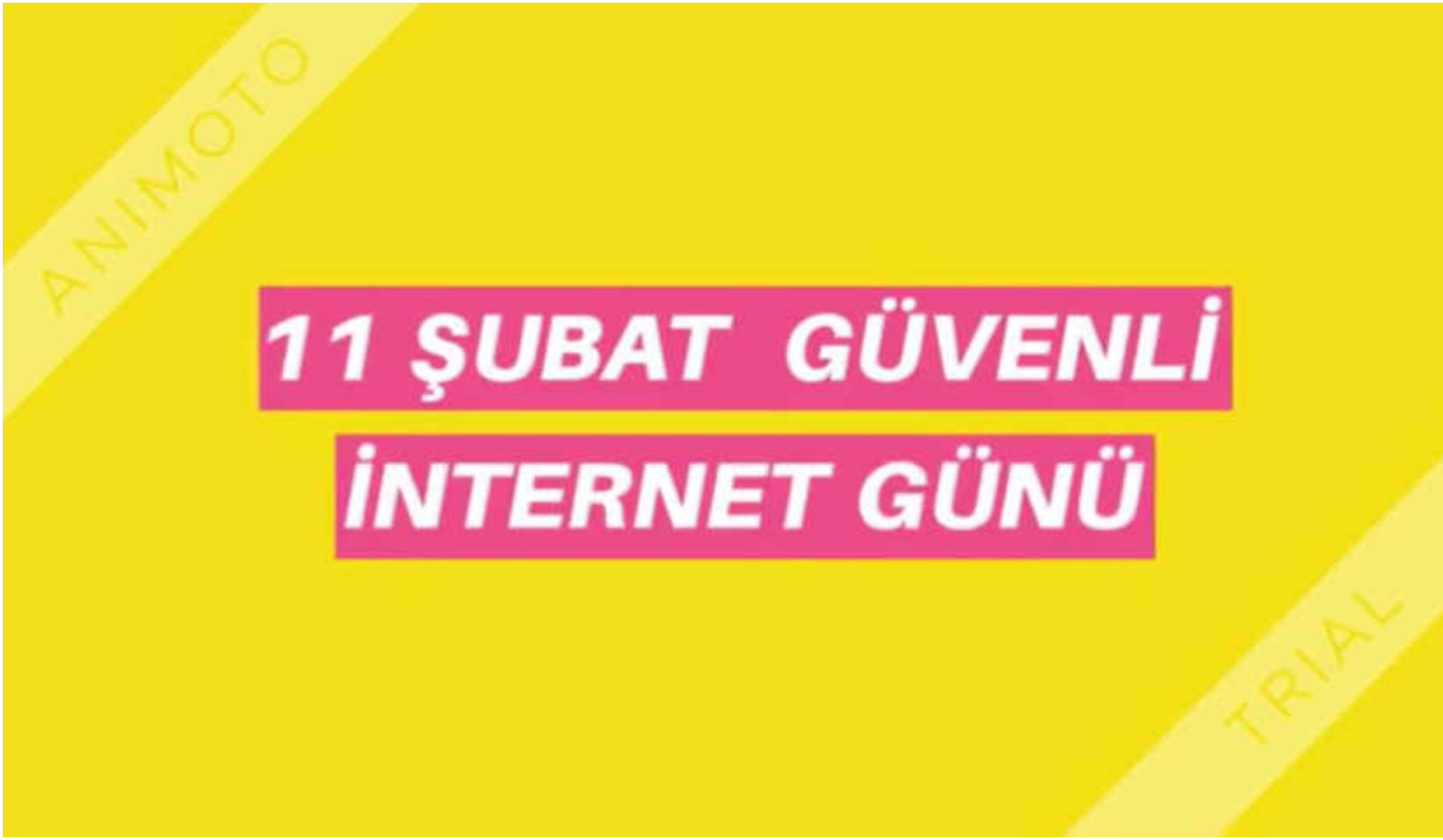
SEFE INTERNET DAY STUDENT ACTIVITIES

ETWINNING PROJELERİNDE GÖREVLİ ÖĞRENCİLERİMİZİN TÜM OKUL ÖĞRENCİLERİNE YAPTIKLARI E-GÜVENLİK SUNUMU

E-SAFETY PRESENTATION BY OUR STUDENTS IN ETWINNING PROJECTS TO ALL SCHOOL STUDENTS


SİBER
TUZAKLAR


güvenli
çocuk



ETWINNING PROJELERİNDE GÖREVLİ ÖĞRENCİLERİMİZİN HAZIRLADIĞI VİDEOLAR

VIDEOS PREPARED BY OUR STUDENTS IN ETWINNING PROJECTS

https://youtu.be/qiHSXgaMbZQ

https://youtu.be/hYEi4xsi6Gc

ETWINNING PROJELERİMİZDE E-GÜVENLİK KONULARI İŞLENMİŞTİR.

E-SAFETY ISSUES ARE PROCESSED IN OUR ETWINNING PROJECTS.

Güvenli İnternet Günü Sanal Panomuz

Erol KESKİN Eskişehir Şehit Teğmen Subutay Alkan Ortaokulu
Projede görevli öğrencilerim Nida Ö. ve D.Kibele D. okulumuz öğrencilerine Güvenli İnternet Günü ile ilgili sunum yaptılar.

Efilay ER[illegible]GLU/Ayten Çağıra[illegible] Ortaokulu Konyaa[illegible]/ANTALYA
Güvenli İ[illegible]rnet Günü Panomu[illegible]

Alev ÖZÇELİK / Amasya Yavuz Selim Ortaokulu
Güvenli internet günü etkinliğimiz

FATMA BİLGE YALAVAÇ/EMİNE BORO ORTAOKULU MERSİN
Güvenli İnternet Günü etkinliğimizi yapıp Panomuzu hazırladık

SELİNAY SAVAŞ Yahya Kemal Beyatlı Ortaokulu
Güvenli İnternet Günü Okul Panomuz

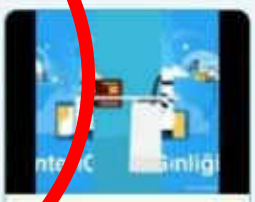
Gökmen KILIÇ -Ahmet Cevdet Çamurdan Ortaokulu
Etwinningonline.eba üzerinden İnternet Güvenliği ve eTwinning Etiği kursumuzu tamamlayıp sertifikamızı aldık

Gökmen KILIÇ -Ahmet Cevdet Çamurdan Ortaokulu
Etwinningonline.eba üzerinden eSafety Label Hakkında Herşey kursumuzu tamamlayıp

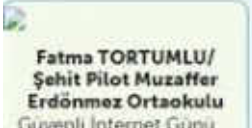
Emine İNANKAÇ Kır[illegible] Şehit Kadir Kayhan

YASEMİN POLAT/ANKA[illegible] MAMAK ŞEHİT H[illegible]SAN ALTIN ORTAO[illegible]LU
güvenli internet kullanımı haftasın[illegible] öğrencilerimiz İlay[illegible] Ö. VE Hatice K. Digital bilgilendirme panosu hazırladı ve sınıf whatsapp gruplarımızda paylaşarak bilgilendirme yaptık.

Erol KESKİN Eskişehir Şehit Teğmen Subutay Alkan Ortaokulu



[illegible]atma TORTUMLU/ Şehit Pilot Muzaffer Erdönmez Ortaokulu
Güvenli İnternet Günü videomuz



Fatma TORTUMLU/ Şehit Pilot Muzaffer Erdönmez Ortaokulu
Güvenli İnternet Günü afişimiz

Fatma TORTUMLU/ Şehit Pilot Muzaffer Erdönmez Ortaokulu
Güvenli İnternet Günü Wordart Çalışmamız

YASEMİN POLAT/ANKARA MAMAK ŞEHİT HASAN ALTIN ORTAOKULU
güvenli internet günü öğrencilerimizin wor ard çalışmaları

CENNET DEDEOLUK
MUHİTTİN GÜZELKILINÇ İHO GÜVENLİ İNTERNET PANOMUZ

Feyza ALAY SADAKATLİ Ertuğrul Gazi Ortaokulu
Güvenli İnternet Günü Panomuz

Sayfalar

F-2/Safer Internet Day's Activities

Safer Internet Day's Acitivities

Aysel YILDIZ-Cemil Meriç Ortaokulu
10-11 Şubat güvenli internet kullanımı ile ilgili panomuzu öğrencilerimizle oluşturduk.

Mimar Sinan İmam Hatip Ortaokulu-Ayşe Nazlı ERGÜN DÖGEN
10-11 Şubat "Güvenli İnternet Kullanımı"günüyle ilgili öğrencilerimiz proje çalışmalarını yaptılar.

Hasibe İnce-Kadınhanı Örnekköy Ortaokulu
10-11 Şubat güvenli internet kullanımı ile ilgili panomuz projede görevli öğrenciler tarafından oluşturuldu.

panomuz
öğrencileri
tarafından hazırlandı.

Erol KESKİN-Eskişehir Şehit Teğmen Subutay Alkan Ortaokulu
Projemizdeki tüm öğrencilerimiz tarafından hazırlanan boyamalar Pano düzenlemesinden sorumlu öğrencilerimiz İlayda A. ve Beren D. tarafından hazırlanan Güvenli İnternet Günü Panomuzda sergilendi

Erol KESKİN-Eskişehir Şehit Teğmen Subutay Alkan Ortaokulu
Proje ekibimizde görevli olan Nida Ö. ve D.Kibele D. tarafından okulumuz öğrencilerine Güvenli İnternet Sunumu yapıldı.

Ebru SAYAK/Hasan Karacalar Ortaokulu
okulumuz eTwinning kulübü ve proje öğrencileri güvenli internet günü panosunu hazırladılar.

Fatma Buket Şahin/Ahmet Hazım Uluşahin İHO
Güvenli İnternet Günü Etkinliğimiz

ÖZGÜL DEVECİ-Lütfiye Ali Şadi Çelik Ortaokulu
Güvenli internet kullanımı konulu panomuz

Cemile BARUT-Ilıdağ Ortaokulu
10-11 Şubat "Güvenli İnternet Kullanımı"günüyle ilgili boyama ve bilgilendirmelerden oluşan panomuz


İNTERNETİN ALTIN KURALLARI
SİBER TUZAKLAR
ÇOCUKLAR DİKKAT!
GÜVENLİ İNTERNET İÇİN

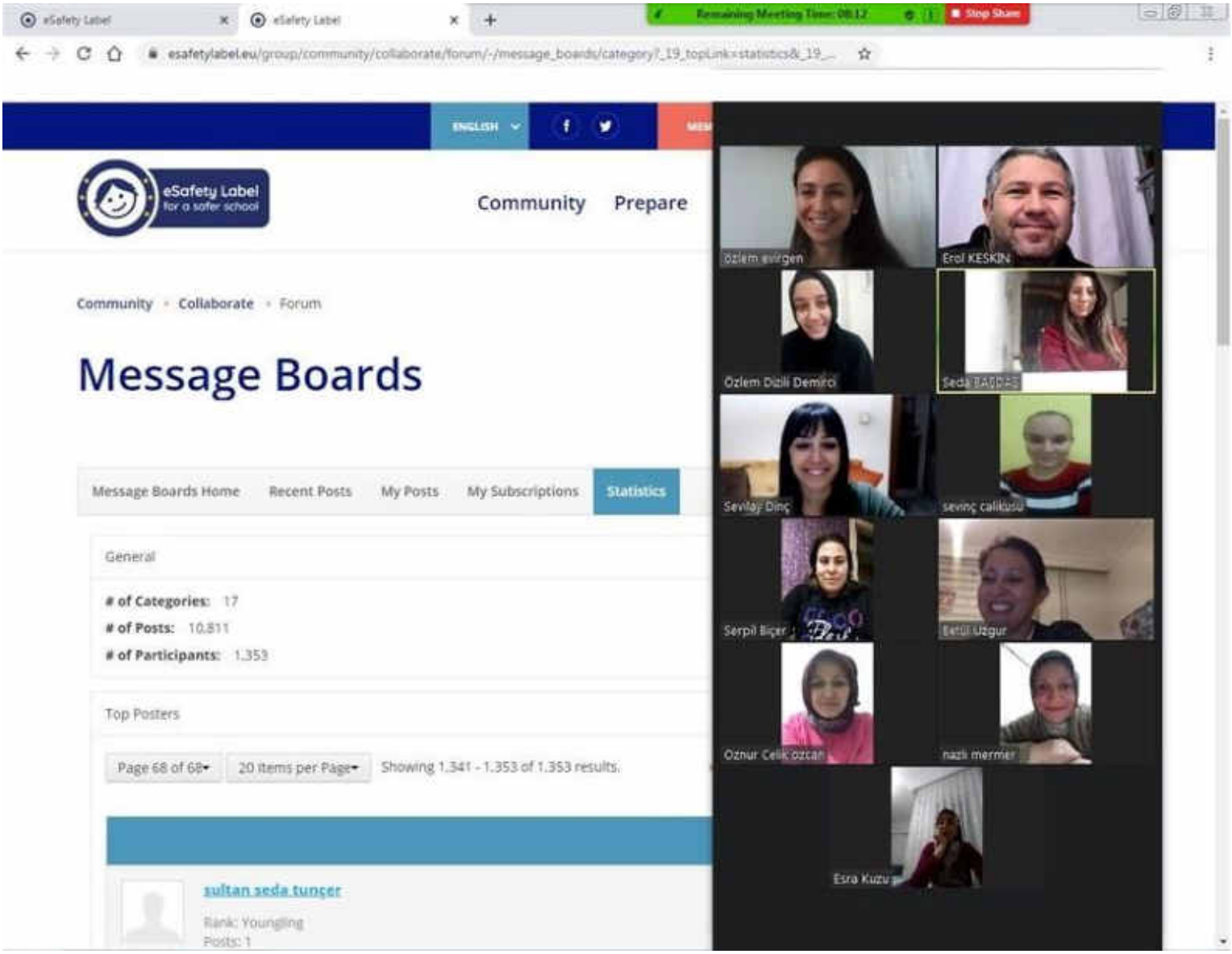

İNTERNETİN ALTIN KURALLARI
SİBER TUZAKLAR
ÇOCUKLAR DİKKAT!
GÜVENLİ İNTERNET İÇİN


İNTERNETİN ALTIN KURALLARI
SİBER TUZAKLAR
eTwinning
ÇOCUKLAR DİKKAT!
GÜVENLİ İNTERNET İÇİN


FİLTRELEME PROGRAMLARI KULLANIN!
BİLGİ PAYLAŞMADAN ÖNCE DÜŞÜN!
11 ŞUBAT GÜVENLİ İNTERNET GÜNÜ 2020
TANIMADIĞIN KİŞİLERLE ARKADAŞLIK KURMAMALISIN!
ŞİFRELERİNİ KİMSEYLE PAYLAŞMA!
KİŞİSEL BİLGİLERİNİ KORU!
İNTERNETTE Kİ ZORBALIKLARA KARŞI OLMALISIN!
SİZE ZORBALIK YAPANLARI AİLENİZLE PAYLAŞIN!
BİLGİSAYARINI VİRÜSLERDEN KORUMALISIN!
TANIMADIĞIN MESAJLARA CEVAP VERME!
İNTERNETTEKİ HERŞEYE SAĞLAMA!
GÜVENLİ İNTERNET İÇİN
ETWINNING KULÜBÜ

ÖĞRETMENLERİMİZLE ONLİNE E-GÜVENLİK TOPLANTIMIZ

OUR ONLINE E-SAFERITY MEETING WITH OUR TEACHERS



Amaç:

Bu politikanın amacı, Bilgi İşlem Dairesi Başkanlığı bünyesindeki her türlü bilginin gizliliğinin, bütünlüğünün ve erişilebilirliğinin korunması ve uygun biçimde yönetilmesidir.

Kapsam:

Bilgi İşlem Dairesi Başkanlığı Bilgi Güvenliği Yönetim Sistemi, Başkanlık tarafından sağlanan ve bilgi içeren her türlü hizmetlerinden doğan yazılı ve elektronik ortamdaki bilgileri kapsar.

Aşağıdakileri sağlamak Bilgi İşlem Dairesi Başkanlığının politikasıdır.

1. Bilgi, izinsiz erişime karşı korunur.
2. Bilgi, yetkisiz kişilere kasten veya dikkatsizlik sonucu verilmez.
3. Yetkisiz kişilerce yapılabilecek değişikliklere karşı korunmak suretiyle bilginin doğru kalması sağlanır.
4. Bilgi, yetkili kişilerin ihtiyaç duydukları anda kolayca erişebilecekleri şekilde hazır bulundurulur.
5. Bilgi Güvenliği konusundaki yasal şartlara uyulur.
6. Tüm çalışanlara, bilgi güvenliği konusunda eğitim verilir.
7. Tespit edilen tüm bilgi güvenliği açıkları ve olası zayıf noktalar, BGYS daire koordinatörüne rapor edilir ve araştırılır. Eğer bu güvenlik açıkları önceden belirlenmiş süre dâhilinde giderilemiyorsa Yönetim Hizmetleri ve Bilgi Güvenliği Dairesi'ne bildirilir.
8. Bilgi İşlem Dairesi Başkanlığının sahip olduğu kullanıcı kimlik bilgileri, personel, öğrenci ve veli bilgileri, yazılım, veri tabanı, sunucu ve bunların üzerlerindeki bilgiler ile istemci bilgisayarlarının güvenliği birincil derecede öncelikli ve koruma altında olan varlıklardır.

9. Bilgi İşlem Dairesi Başkanlığı Bilgi Güvenliği Yönetim Sisteminin etkin bir şekilde yürütülmesi ve sürekli izlenip iyileştirilmesi için gerekli desteği verecek, eğitimler ve güvenlik önlemlerine yönelik kaynak sağlayacaktır.

Uygulanabilirlik:

Bilgi Güvenliği Yönetim Sistemi; Bilgi İşlem Dairesi Başkanlığı'nca belirlenen hedefler doğrultusunda, başkanlık personeli ve başkanlık kapsamında bulunan varlıklarla herhangi bir şekilde ilgisi olan tüm paydaşlar bu politikayı uygulamakla yükümlüdürler ve politikayı onaylamış olan MEB Bilgi İşlem Dairesi Başkanlığının desteğine sahip olacaklardır.

Uygulama

1. Uygun risk değerlendirmesi aracılığıyla varlıkların değeri tespit edilir, açıklıkları ve tehditleri Risk Değerlendirme Prosedürü'ne göre belirlenir.

2. Risk değerlendirme sürecinde ortaya çıkan açıkları, Risk Yönetim Prosedürü doğrultusunda en aza indirilir. Resmî bir "Bilgi Güvenliği Yönetim Sistemi"nin tasarlanması, uygulanması ve sürdürülmesi aracığıyla, açığa çıkabilecek riskler kabul edilebilir düzeylere indirilir.

3. Bilgi Güvenliği Yönetim Sistemi sürdürülürken aşağıda belirtilen kanunlara çerçevesinde hareket edilir.

    - 652 sayılı Millî Eğitim Bakanlığının Teşkilat ve Görevleri Hakkında Kanun Hükmünde Kararname
    - 5846 sayılı Fikrî Mülkiyet Hakları Kanunu
    - 5237 sayılı Türk Ceza Kanunu
    - 5651 Sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkındaki Kanun

4. Bilgi Güvenliğiyle ilgili tüm üçüncü taraflarla imzalanmış protokol ve/veya sözleşme hükümlerine uygun davranılır.

5. Bilgi İşlem Dairesi Başkanlığının tüm politika, prosedür ve talimatlarına uygun davranılır.

6. TS ISO IEC 27001 uygunluğuna bağlı kalınır.

Destek Politikalar ve Prosedürler:

1. Eğitim Politikası,
2. İş Sürekliliği Politikası,
3. Kayıt Tutma Politikası,
4. Yedekleme Politikası,
5. İnternet Kullanım Politikası,
6. Ağ Hizmetleri Politikası,
7. e-Posta Politikası,
8. Erişim Denetim Politikası,
9. Teknik Destek Politikası,
10. Temiz Masa ve Temiz Ekran Politikası,
11. Web Barındırma Hizmeti Politikası,
12. Yazılım Hizmetleri Politikası,
13. Bilgi ve Yazılım Değişimi Politikası,

Sorumlular:

1. Bilgi İşlem Dairesi Başkanlığı bu politikayı oluşturur ve gözden geçirir.
2. Bilgi Güvenliği Yöneticisi, uygun standartlar ve prosedürler aracılığı ile bu politikanın uygulanmasını destekler.

3. Tüm personel, Bilgi Güvenliği Politikasını sürdürmek için hazırlanan politika prosedürlere uyar.

4. Tüm personel, güvenlik olaylarını raporlamaktan ve tespit edilen zayıf noktaları bildirmekten sorumludur.

5. Bilgi İşlem Dairesi Başkanlığı kapsamında bulunan varlıklarla herhangi bir şekilde ilgisi olan tüm paydaşlar bu politikayı uygulamakla sorumludurlar.

6. Bilgi İşlem Dairesi Başkanlığına ya da üçüncü taraflara ait bilgilerin güvenliğini tehlikeye atacak herhangi bir kasti hareket, disiplin cezasına ve/veya hukuki önleme tabidir.

Gözden Geçirme:

Bu politika, yılda en az bir kere düzenli olarak, önemli güvenlik arızaları, yeni güvenlik açıkları, kurumsal veya teknik altyapı değişiklikleri ile ilgili kontroller baz alınarak yönetim tarafından gözden geçirilir ve hizmet etme becerimize uygun olmasını sağlamak üzere gerek duyulduğunda değiştirilir.

T.C.
MİLLÎ EĞİTİM BAKANLIĞI
Bilgi İşlem Dairesi Başkanlığı

Sayı : 49473396/703.03/7180248 10.07.2015
Konu: İnternet ve Bilgi Güvenliği

İlgi: a) Bilgi İşlem Dairesi Başkanlığının 27/02/2014 tarihli ve 49473396/703.03/861980 sayılı yazısı.
b) 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun.
c) 11.04.2012 tarihli ve 565 sayılı Millî Eğitim Bakanlığı Bilgi ve Sistem Güvenliği Yönergesi.

Bakanlık olarak, temel amaçlarımızdan biri, hizmet verdiğimiz tüm kesimler için, güvenli ve kesintisiz ağ hizmetini sağlamaktır. Bu amaçla; gerçekleşmesi olası tehditlere karşı, iç ağdaki trafiği ve internet trafiğini sağlıklı yönetebilmek için güvenlik duvarı, saldırı tespit ve koruma sistemleri, içerik filtreleme, spam analizi, antivirüs vb. ürün ve uygulamaları kullanılmaktadır.

11 Nisan 2012 tarihinde ilgi (c) de yer alan Bilgi ve Sistem Güvenliği Yönergesi çıkarılmıştır. Bu yönerge ile kurum çalışanlarımıza, sistem ve bilgi güvenliği kapsamında, uyulması gereken kurallar, olması ve olmaması gereken tasarruflar açıklanmıştır. Bilgi ve sistem güvenliği anlamında kurum politikalarını hiçe sayma, uygulanan filtreleme çözümlerini delme, gereksiz yüksek trafik oluşturma, güvensiz yazılım kullanma vb. gibi durumlar oluşabilmektedir. İlgi yönergenin 11. maddesinin 4. bendinde belirtildiği gibi "Telif hakları ve lisansları ihlal eden, Bakanlık ağında yoğun ağ trafiğine sebep olan, iki veya daha fazla kullanıcı arasında veri paylaşmak için kullanılan noktadan noktaya (Peer-to-peer - P2P) uygulamalar kullanılamaz. Dosya paylaşımı, anlık mesajlaşma programları ve yoğun ağ trafiğine sebep olan uygulamalar gerekli görüldüğünde Bakanlık tarafından filtrelenir." denilmektedir. Bu sebeple Bakanlık TTVPN ve MEB ADSL hattını kullanan kullanıcıların (İl ve İlçe Müdürlükleri, Resmi Kurumlar, Okullar) uygulanan güvenlik politika ve kuralları çerçevesinde davranmaları gerekmektedir.

Oluşturulan bilgi güvenliği politikaları gereği başta merkez teşkilatlarımız olmak üzere bakanlığımız üzerinden hizmet alan tüm alt kurumlarımız bu politikalara tabidir. Bu anlamda merkez teşkilatlarda bulunan kullanıcılarımızın kaçınması gereken hususlar şu şekilde sıralanabilir: Kurumsal ağ dışında bağımsız bir internet hattına veya başka bir ağa katılmak, (ADSL, VDSL, wireless, 3G, vb.) kurum içinde kullanılan kullanıcı adı ve şifre bilgilerinin üçüncü kişilerle paylaşmak, çeşitli proxy programları ile meb güvenlik hizmetlerini atlatmaya çalışmak, farklı yazılımlar veya donanımlar yardımı ile meb sistemlerine, kurumsal ağ altyapısına saldırmak ve verilen hizmetleri kesintiye uğratmak veya uğratmaya çalışmak.

Atatürk Blv. 06648 Kızılay/ANKARA
Elektronik Ağ: https://bidb.meb.gov.tr
e-posta: bidb@meb.gov.tr

Ayrıntılı bilgi için: M.KARADAĞ - Daire Bşk.
Tel: (0 312) 413 11 96
Faks: (0 312) 417 50 09

Bakanlığımız 2012 yılından itibaren İl Milli Eğitim Müdürlüklerini TTVPN Metro İnternet Projesine dahil etmiştir Bu süreç ile birlikte İl Milli Eğitim Müdürlüklerimizde ve ek binalarda yer alan ADSL, VDSL gibi bağlantıların iptal edilmesi ilgi (a) yazıda istenmiştir. Bu kapsamda İl Milli Eğitim Müdürlüklerinin Ağ alt yapıları yenilenmiş ve merkezi yönetime geçilmiştir. Son zamanlarda yapılan incelemelerde İl Milli Eğitim Müdürlüklerimiz bünyesinde kurum, şahsi veya benzeri yöntemlerle ADSL, VDSL, 3G, wireless gibi bağlatıların yapıldığı tespit edilmiştir.

Bu sebeple İl Millî Eğitim Müdürlüğü bünyesinde yer alan Bakanlık hattı haricindeki tüm internet hatlarının (ADSL, VDSL 3G, Wireless vb.) acilen iptal edilmesi, gelecekte Bakanlığın ilgili birimlerinin bilgisi olmadan bu ve benzeri bağlantılara izin verilmemesi ile belirtilen bağlantıları iptal ettirmeme konusunda ısrarcı davranış sergileyen personel veya kurum hakkında ilgi (a) da belirtilen yasal sürecin başlatılması gerekmektedir.

Ayrıca 2014 yılında yapılan iyileştirmelerle MEB ADSL VE MEB VDSL hızları güncellenmiştir. İlçe Milli Eğitim Müdürlükleri, Resmi Kurumlar ve Okullarımızda MEB ADSL /VDSL hattı kullanılması zorunludur. Her ne şekilde olursa olsun (kişisel,okul aile birliği vb.) ADSL, 3G vb. hat kullanmak yasaktır. İhtiyaç durumunda 2. MEB ADSL hattı temin edilebilir. Aksi davranış tespit edilen personel vaya kurum hakkında gerekli yasal süreç başlatılacaktır. Halka hizmet veren kurumlar (Hizmetiçi Eğitim Enstitüsü, Öğretmenevi ve Halk Eğitim Merkezi) idari işlemler haricinde kapsam dışında tutulabilir. Resmi kurumlarımızın kullandıkları ADSL, 3G ve benzeri hatlar; adres bilgisi, abonelik gibi bilgilerle operatörlerden sorgulanarak kontrol edilmektedir.

Oluşması muhtemel bilişim suçlarının önüne geçebilmek amacıyla yukarıda belirtilen çalışmaların acilen tamamlanarak, birimlerinizde çalışan personelin, sözü edilen ilgili Kanun ve Yönerge doğrultusunda tekrar bilgilendirilmesi hususunda;

Bilgilerinizi ve gereğini arz/rica ederim.

Bilal TIRNAKÇI
Bakan a.
Bilgi İşlem Dairesi Başkanı

EK:
1.EK-1 İnternet ve Bilgi Güvenliği konulu yazı
2.EK-2 Bilgi ve Sistem Güvenliği Yönergesi

DAĞITIM:
A ve B Planı

Atatürk Blv. 06648 Kızılay/ANKARA
Elektronik Ağ: https://bidb.meb.gov.tr
e-posta: bidb@meb.gov.tr

Ayrıntılı bilgi için: M.KARADAĞ - Daire Bşk.
Tel: (0 312) 413 11 96
Faks: (0 312) 417 50 09

T.C.
MİLLÎ EĞİTİM BAKANLIĞI
Öğretmen Yetiştirme ve Geliştirme Genel Müdürlüğü

Sayı : 43501582/774.01/2494212 16/09/2013
Konu: FATİH Projesi Bilişim Teknolojilerinin ve İnternetin Bilinçli, Güvenli Kullanımı Semineri

İlgi : a) Milli Eğitim Bakanlığı ile Bilgi Teknolojileri ve İletişim Kurumu arasında imzalanan 21 Mayıs 2012 tarihli Protokol.
b) 28.08.2013 tarih ve 30706984/774/2237778 sayılı yazı.

FATİH Projesi kapsamında bilişim teknolojilerinin ve internetin bilinçli, güvenli kullanımı konusunda öğrenci, öğretmen ve ebeveynlerde farkındalığın arttırılması amacıyla ilgi (a) protokol imzalanmıştır.

Protokol doğrultusunda FATİH Projesi Bilişim Teknolojilerinin ve İnternetin Bilinçli, Güvenli Kullanımı Seminerleri düzenlenmiş olup, seminerlere katılan öğretmenler illerinde açılacak olan bu seminerlerde eğitim görevlisi olarak görevlendirilecektir.

Seminerlere resmi okullarda görev yapan tüm öğretmenler katılacaktır.

Bu çerçevede;

1- FATİH Projesi Bilişim Teknolojilerinin ve İnternetin Bilinçli, Güvenli Kullanımı Semineri" faaliyetine alınacak öğretmenlerin tespiti Hizmetiçi Eğitim Şubelerince, eğitimde FATİH Projesinden sorumlu şube müdürü ve Bilişim Teknolojisi İl Koordinatörü işbirliğinde yapılacak ve eğitimler bu doğrultuda planlanacaktır.

2- Proje kapsamında uygulanacak seminer faaliyetinin; günlük 5 saati geçmeyecek şekilde ve mümkün olduğunca mesai saatleri içerisinde yapılacaktır.

3- Okul müdürlükleri tarafından öğretmenlerin proje kapsamındaki eğitimlere katılımlarının sağlanması ve eğitime katılacak öğretmenlerin, eğitim sürecince ders programları ile ilgili gerekli tedbirler alınacaktır.

Eğitimlerde uygulanacak "FATİH Projesi Bilişim Teknolojilerinin ve İnternetin Bilinçli, Güvenli Kullanımı Semineri" programı (EK-1), eğitimlerde görevlendirilecek eğitim görevlileri listesi (EK-2) ve protokol (EK-3) ekte sunulmuştur.

Milli Müdafaa Cad. 6/4 Kızılay/ANKARA
Elektronik Ağ: www.oyegm.meb.gov.tr
e-posta: oyy_meslekiegitim@meb.gov.tr
Ayrıntılı bilgi için:
Tel: (0 312) 417 50 70 /4176
Faks: (0 312) 419 62 74

Yazımız ve ekleri Öğretmen Yetiştirme ve Geliştirme Genel Müdürlüğünün http://oyegm.meb.gov.tr. adresinde yayınlanacaktır.

Herhangi bir aksaklığa meydan vermeden söz konusu mesleki gelişim faaliyetlerinin gerçekleştirilmesi hususunda gereğini rica ederim.

Ömer BALIBEY
Bakan a.
Genel Müdür

EKLER:
EK-1 Mesleki Gelişim Programı (2 sayfa)
EK-2 Eğitim Görevlisi Listesi (11 sayfa)
EK-3 Protokol (3 sayfa)

DAĞITIM:
Gereği :
B Planı

Bilgi :
Yenilik ve Eğitim Teknolojileri Genel Müdürlüğü

Milli Müdafaa Cad. 6/4 Kızılay/ANKARA
Elektronik Ağ: www.oyegm.meb.gov.tr
e-posta: oyg_meslekiselisim@meb.gov.tr

Ayrıntılı bilgi için:
Tel: (0 312) 417 50 70 /4176
Faks: (0 312) 419 62 74

EK-1

T.C.
MİLLÎ EĞİTİM BAKANLIĞI
Öğretmen Yetiştirme ve Geliştirme Genel Müdürlüğü

MESLEKİ GELİŞİM PROGRAMI

1-ETKİNLİĞİN ADI

"Fatih Projesi Bilişim Teknolojilerinin ve İnternetin Bilinçli, Güvenli Kullanımı Semineri"

2-ETKİNLİĞİN AMAÇLARI

Bu faaliyeti başarı ile tamamlayan her kursiyer,

- Eğitimde BT'nin bilinçli ve güvenli kullanımını sağlar,
- İnternetin bilinçli ve güvenli kullanımını sağlar,
- İnternetin kullanımında karşılaşılabilecek risklerden haberdar olur,
- İnternetin ve BT'nin kullanımında hukuki, insani ve teknik boyutu hakkında bilgi sahibi olur,
- BT'nin bilinçli, güvenli kullanımının sağlık boyutundan haberdar olur,
- İnternet bağımlılığı ve elektromanyetik etkilerinden haberdar olur,
- BT'nin ve internetin psikososyal boyutu hakkında bilgi sahibi olur,
- İnterneti daha etkin ve etik kurallara uygun olarak kullanır,
- Dijital vatandaşlık konusunda öğrencilere rehberlik yapar,
- İnternet ortamında işlenebilecek suçlar hakkında bilgi sahibi olur ve öğrencilere rehberlik yapar,
- Bilinçli ve Güvenli internet kullanımı konusunda öğrencilere rehberlik yapar.

3-ETKİNLİĞİN SÜRESİ

Seminerin süresi 10 saattir.

4-ETKİNLİĞİN HEDEF KİTLESİ

T.C. Millî Eğitim Bakanlığına bağlı resmi okullarda görev yapan tüm öğretmenler.

5-ETKİNLİĞİN UYGULAMASI İLE İLGİLİ AÇIKLAMALAR

1. Bu faaliyet okullarda görev yapan tüm öğretmenlere yöneliktir.
2. Bu faaliyet Milli Eğitim Bakanlığı Hizmetiçi Eğitim Yönetmeliği hükümlerine göre yürütülecektir.
3. Fatih Projesi BT'nin Bilinçli, Güvenli Kullanımı Seminerinin gerçekleşeceği salonda İnternet bağlantısının olması esastır.

6-ETKİNLİĞİN İÇERİĞİ

	KONULAR	SÜRE
A	**BT'nin Bilinçli, Güvenli Kullanımının Teknik Boyutu**	**3 Saat**
	1. BT Sistemlerinin Etkin Kullanımı 2. BT'nin Bilinçli Kullanımı 3. BT'nin Güvenli Kullanımı 4. BT'nin Etik Kullanımı 5. Sosyal Ağlarda Karşılaşılacak Riskler ve Çözüm Önerileri 6. E-posta Kullanırken Karşılaşılabilecek Riskler ve Çözüm Önerileri	

	7. İnternet Kullanılırken Karşılaşılabilecek Riskler ve Çözüm Önerileri	
B	**BT'nin Bilinçli, Güvenli Kullanımının Hukuki Boyutu**	**2 Saat**
	1. İnternet Ortamında İşlenebilecek Suçlar 2. Bilişim Suçları İle İlgili Hukuki Düzenlemeleri (Dünya -Türkiye) 3. Bilişim Suçları İle Yaptırımlar 4. Bilişim Suçlarında Takip Edilecek Prosedür 5. Faili Bulma Prosedürü 6. Bilişim Suçlarına Karşı Alınması Gereken Önlemler	
C	**BT'nin Bilinçli, Güvenli Kullanımının Eğitim Boyutu**	**3 Saat**
	1. Dijital Vatandaşlık Kavramı 2. Çocuk ve Gençlerin internetle Tanışması 3. Okullarda İnternet Kullanımı 4. Sosyal Ağlar 5. Sohbet Odaları 6. İnternette Rol Modellik ve Özenti 7. Teknoloji Bağımlılığı 8. Saldırganlık/Hırçınlık 9. Mobil İnternet Kullanımı ve Sexting 10. Siber Zorbalık	
D	**BT'nin Bilinçli, Güvenli Kullanımının Sağlık boyutu**	**1 Saat**
	1. Bilişim Uygulamalarına Uygun Olarak Ortaya Çıkan Sağlık Sorunları 2. Bilişim Teknolojilerini Kullanım Süresi ve Sıklığı 3. Bilişim Teknolojilerinin Elektromanyetik Etkisi 4. Bilişim Teknolojilerinin Sağlık Alanında Etkin Kullanılması 5. Çocukların Gelişim Dönemlerine Göre Ailelerin Tutumu 6. İnternet Bağımlılığının Sağlık Boyutu 7. Siber Ortamda Doğru Sağlık Bilgisine Ulaşma 8. Organik, Bilişsel, Psikososyal Riskler ve Korunma	
E	**BT'nin Bilinçli, Güvenli Kullanımının Psikososyal Boyutu**	**1 Saat**
	1. Bireyin Psikososyal Özellikleri Üzerinde İnternet'in Etkisi 2. İletişim Düzeyleri Üzerindeki Etkisi 3. Kişilik Özellikleri İle İlişkisi 4. Bağımlı Kişilik ve İnternet Bağımlılığı	
	TOPLAM	**10 Saat**

7. ÖĞRETİM YÖNTEM TEKNİK ve STRATEJİLERİ

1. Eğitime katılan kursiyerlere program içeriği ve ders materyalleri elektronik ortamda verilecektir.
2. Öğretim sürecinde etkili katılımı sağlamak için sunum, tartışma, soru-cevap yöntemlerine yer verilecektir.

8. ÖLÇME VE DEĞERLENDİRME

3. Milli Eğitim Bakanlığı Hizmetiçi Eğitim Yönetmeliği doğrultusunda katılımcılara "Seminer Katılım Sertifikası" verilecektir.

BTK
BİLGİ TEKNOLOJİLERİ
VE İLETİŞİM KURUMU

PROTOKOL

MİLLİ EĞİTİM BAKANLIĞI İLE BİLGİ TEKNOLOJİLERİ VE İLETİŞİM KURUMU ARASINDA DÜZENLENEN İŞBİRLİĞİ PROTOKOLÜ

AMAÇ

Madde 1: Bu protokolün amacı, Milli Eğitim Bakanlığı ile Bilgi Teknolojileri ve İletişim Kurumu arasında, İnternetin güvenli kullanımı bilincinin yaygınlaştırılması için yapılacak işbirliğinin ve ortak hizmetlerin çerçevesini belirtmektir. Bu protokol ile Milli Eğitim Bakanlığı bünyesinde eğitim gören ilk ve orta öğretim kademelerindeki tüm öğrenciler, öğretmenler, idareciler ve velilerin daha bilinçli bir İnternet kullanıcısı olmalarına destek sağlanması amaçlanmaktadır.

KAPSAM

Madde 2: Bu protokol, Milli Eğitim Bakanlığı ile Bilgi Teknolojileri ve İletişim Kurumu'nun birlikte kararlaştırdığı ve birlikte gerçekleştirilecek faaliyetleri kapsar.

DAYANAK

Madde 3

3.1. Anayasa'nın "Ailenin Korunması ve Çocuk Hakları" başlıklı 41. Maddesi; "...Devlet, ailenin huzur ve refahı ile özellikle anaların ve çocukların korunması... için gerekli tedbirleri alır..." hükmü,

3.2. Anayasa'nın "Gençliğin korunması" başlıklı 58. Maddesi; "Devlet, gençleri alkol düşkünlüğünden, uyuşturucu maddelerden, suçluluk, kumar ve benzeri kötü alışkanlıklardan ve cehaletten korumak için gerekli tedbirleri alır." hükmü,

3.3. 1739 sayılı Millî Eğitim Temel Kanununun Genel Amaçlar başlığını taşıyan 2. Maddesi 2. fıkra; "Türk Milli Eğitiminin genel amacı, Türk Milletinin bütün fertlerini; Beden, zihin, ahlak, ruh ve duygu bakımlarından dengeli ve sağlıklı şekilde gelişmiş bir kişiliğe ve karaktere, hür ve bilimsel düşünme gücüne, geniş bir dünya görüşüne sahip, insan haklarına saygılı, kişilik ve teşebbüse değer veren, topluma karşı sorumluluk duyan; yapıcı, yaratıcı ve verimli kişiler olarak yetiştirmek;" hükmü,

3.4. 4.5.2007 Tarihli ve 5651 Sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanunun 10.Madde 4. fıkrası: "Başkanlığın bu Kanun kapsamındaki görev ve yetkileri şunlardır: a) Bakanlık, kolluk kuvvetleri, ilgili kamu kurum ve kuruluşları ile içerik, yer ve erişim sağlayıcılar ve ilgili sivil toplum kuruluşları arasında koordinasyon oluşturarak internet ortamında yapılan ve bu Kanun kapsamına giren suçları oluşturan içeriğe sahip faaliyet ve yayınları önlemeye yönelik çalışmalar yapmak;" hükmü.

3.5. Çocuk Haklarına Dair Sözleşme

TANIMLAR

Madde 4: Bu protokolde geçen;

MEB: Milli Eğitim Bakanlığı'nı,

BTK: Bilgi Teknolojileri ve İletişim Kurumu'nu,

INSAFE: Avrupa Güvenli İnternet Merkezleri Ağı'nı, ifade eder.

Eğitimde Fatih Projesi: Eğitimde Fırsatları Artırma Teknolojiyi İyileştirme Hareketi

TARAFLAR

Madde 5: Bu protokol, Milli Eğitim Bakanlığı (MEB) ile Bilgi Teknolojileri ve İletişim Kurumu (BTK) arasında düzenlenerek taraflarca imza altına alınmıştır.

TEBLİGAT ADRESLERİ

Madde 6: Tarafların adres ve telefonları aşağıdaki gibidir:

Milli Eğitim Bakanlığı (MEB)
Atatürk Bulvarı Bakanlıklar Çankaya/ANKARA
Tel:(312) 419 14 10 Faks: (312) 417 70 27

Bilgi Teknolojileri ve İletişim Kurumu (BTK)
Yeşilırmak sokak No:16 Demirtepe/ANKARA
Tel: (312) 294 72 00 Faks : (312) 294 71 45

FAALİYETLER

Madde 7: Eğitimde Fatih Projesi'nin "Bilinçli, Güvenli, Yönetilebilir ve Ölçülebilir BT ve İnternet Kullanımı" bileşeni ile "Güvenli İnternet Hizmeti" ne yönelik aşağıda belirtilen konularda işbirliği yapılması kararlaştırılmıştır:

7.1. Eğitimde Fatih Projesi kapsamında öğrencilere dağıtılacak tablet bilgisayarlarla beraber INSAFE tarafından hazırlanan ve BTK tarafından Türkçe'ye uyarlanan "aile e-güvenlik seti"nin, taraflarca düzenlendikten sonra dağıtılması için çalışmalar yapılacaktır.

7.2. Eğitimde Fatih Projesi'nin "Bilinçli, Güvenli, Yönetilebilir ve Ölçülebilir BT ve İnternet Kullanımı" bileşeni ile ilgili olarak idarecilere ve Eğitimde Fatih Projesi eğitmenlerine seminerler düzenlenecektir. Söz konusu seminerler için, İnternetin Güvenli Kullanımı ile ilgili konularda BTK ve MEB tarafından oluşturulacak akademik ve uzman çalışma grupları yardımıyla içerikler hazırlanacaktır.

7.3. Eğitimde Fatih Projesi'nin "Bilinçli, Güvenli, Yönetilebilir ve Ölçülebilir BT ve İnternet Kullanımı" bileşeni ve BTK'nın "Güvenli İnternet Hizmeti"nin tanıtımı için sinevizyon ve kısa film vb. çalışmalar yapılacaktır.

7.4. Her yıl düzenlenen Güvenli İnternet Günü etkinliklerinin birlikte kutlanması için çalışmalar yapılacaktır. Düzenlenecek konferans, panel ve açık oturumlara ihtiyaç halinde BTK tarafından uzmanların, akademisyenlerin, sektör ve sivil toplum temsilcilerinin katılması temin edilecektir.

7.5. İnternetin Güvenli Kullanımı ile ilgili sayısal içerikler hazırlanarak, bu içeriklerin öğrencilere dağıtılacak tablet bilgisayarlarda yer alması sağlanacaktır.

7.6. İnternetin Güvenli Kullanımına ilişkin konularda BTK tarafından oluşturulan akademik ve uzman çalışma gruplarının hazırlayacağı müfredat taslağı MEB'e sunulacaktır. İhtiyaç duyulması halinde MEB tarafından müfredatta yer almasına yönelik çalışmalar yapılacaktır.

SÜRE

Madde 8: İşbu Protokol tarafların karşılıklı mutabık kalacakları sürece devam eder.

DİĞER HUSUSLAR

Madde 9: İşbu Protokolün uygulanması sırasında tespit edilecek diğer hususlar (basın duyurusu, masraflar vb.) MEB ile BTK arasında karşılıklı görüşmelerle düzenlenecektir.

YÜRÜRLÜK

Madde 10: İşbu Protokol on maddeden ibaret olup, iki nüsha halinde düzenlenmiş ve taraflarca …./05/2012 tarihinde imzalanmıştır.

Dr. Tayfun ACARER
Kurul Başkanı
Bilgi Teknolojileri ve İletişim Kurumu

M. Emin ZARARSIZ
Müsteşar
Milli Eğitim Bakanlığı

T.C.
MİLLÎ EĞİTİM BAKANLIĞI
Bilgi İşlem Dairesi Başkanlığı

Sayı : 76884643-20-E.10943576 05.06.2018
Konu : Okul İnternet Siteleri Yönergesi Taslağı

BAKANLIK MAKAMINA

Millî Eğitim Bakanlığına bağlı devlet okulları ve meb.k12.tr alan adını kullanan kurumların kurumsal internet sitelerinin hizmet başvurusu, yönetimi ve yayını hususunda uyulması gereken usul ve esasları belirlemek amacıyla Okul İnternet Siteleri Yönergesi taslağı hazırlanmıştır.

Okul İnternet Siteleri Yönergesi taslağının Makamlarınızca da uygun görülmesi halinde yürürlüğe girmesi hususunu olurlarınıza arz ederim.

Özgür TÜRK
Bilgi İşlem Dairesi Başkanı V.

Ek: Yönerge Taslağı (3 sayfa)

Uygun görüşle arz ederim.

Yusuf TEKİN
Müsteşar

OLUR
05.06.2018

İsmet YILMAZ
Bakan

Adres: MEB Bilgi İşlem Dairesi Başkanlığı
Elektronik Ağ: bidb.meb.gov.tr
e-posta: skamsiz@meb.gov.tr

Bilgi için: Sevim KAMSIZ
Tel: (0312) 413 12 03
Faks: (0312) 417 50 09

T.C.
MİLLÎ EĞİTİM BAKANLIĞI
OKUL İNTERNET SİTELERİ YÖNERGESİ

BİRİNCİ BÖLÜM
Amaç, Kapsam, Dayanak ve Tanımlar

Amaç
MADDE 1 – (1) Bu Yönergenin amacı, Millî Eğitim Bakanlığına bağlı devlet okulları ve meb.k12.tr alan adını kullanan kurumların kurumsal internet sitelerinin hizmet başvurusu, yönetimi ve yayını hususunda uyulması gereken usul ve esasları belirlemektir.

Kapsam
MADDE 2 – (1) Bu Yönerge, Millî Eğitim Bakanlığına bağlı devlet okulları ve meb.k12.tr alan adını kullanan kurumları kapsar.

Dayanak
MADDE 3 – (1) Bu Yönerge, 652 sayılı Millî Eğitim Bakanlığının Teşkilat ve Görevleri Hakkında Kanun Hükmünde Kararnameye dayanılarak hazırlanmıştır.

Tanımlar ve kısaltmalar
MADDE 4 – (1) Bu Yönergede geçen;
a) Bakanlık: Millî Eğitim Bakanlığını,
b) Başkanlık: Bilgi İşlem Dairesi Başkanlığını,
c) Panel: mebk12 Yönetim Panelini,
ç) Panel yetkilisi: mebk12 Yönetim Paneline giriş yetkisi bulunan kullanıcıları,
d) Hedef kitle: Okul veya kurumun öğrenci, veli, öğretmen ve çalışanlarını,
e) İnternet sitesi: Okul veya kurumun internet sitesini,
f) Yönerge: Okul internet siteleri kullanım yönergesini ifade eder.

İKİNCİ BÖLÜM
Sorumluk

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, meb.k12.tr internet site yönetim sistemi iz kayıtları ve internet site erişim kayıtları, iz toplama yöntemleri kullanılarak toplanır. Bu kayıtlar, ilgili mevzuatında belirlenen süreyle Başkanlıkça saklanır. Başkanlıkça bu bilgiler istatistik, raporlama ve inceleme amaçlı olarak kullanılabilir.
(2) İl/ilçe millî eğitim müdürlüklerince okul ve kurumlara internet sitesi yönetimi ve yayını ile ilgili bilgilendirme yapılır.
(3) İnternet sitelerinin Yönergeye uygunluğu il/ilçe millî eğitim müdürlüklerince denetlenir ve internet sitesi bulunmayan okulların internet sitesi oluşturulması sağlanır.
(4) Kapatılan okul ve kurumların internet siteleri, il/ilçe millî eğitim müdürlüklerince silinir.

ÜÇÜNCÜ BÖLÜM
Uygulama Esasları

İnternet sitesi hizmet başvurusu
MADDE 6 – (1) Okul müdürü, internet sitesi hizmetini başlatmak için www.meb.k12.tr adresindeki başvuru formu üzerinden kurum MEBBİS kullanıcısı ile hizmet tahsis başvurusu yapar. Alan adı belirlenirken okul adını temsil eden kısa ifade seçilir.

İnternet sitesi yayın ekibi, kuruluşu ve görevleri
MADDE 7 – (1) İnternet sitesinin işletimi ile ilgili iş ve işlemleri yürütmek üzere okul müdürlüğünce internet yayın ekibi oluşturulur.
(2) İnternet yayın ekibinde görev alacak üyeler, eğitim ve öğretim yılı başında yapılan öğretmenler kurulu toplantısında belirlenir. Öğretmenler kurulunca belirlenecek internet sitesi yayın ekibi üyeleri;
a) İnternet sitesi yayın ekibi yöneticisi: Okul müdürü, müdür başyardımcısı veya bir müdür yardımcısı,
b) İnternet sitesi yöneticisi: Fatih Projesi BT rehber öğretmeni veya bilişim teknolojileri öğretmeni,

c) Editör: Türkçe veya Türk dili ve edebiyatı öğretmeni,
ç) Danışman: Rehberlik öğretmeninden oluşur.

(3) Gerekli görüldüğü durumda diğer alanlardan da görevlendirme yapılır. Öğretmen sayısı yetersiz olan okullarda bir kişi birden fazla görevi yürütür.

(4) İnternet sitesi yayın ekibi yöneticisince, ihtiyaç halinde internet sitesi yayın ekibine yeni görevlendirme yapılır.

(5) İnternet sitesi yayın ekibinin görevleri şunlardır:
a) Okul internet sitesini yayınlar, yönetir.
b) Panel Kullanım ve İçerik Yönetim politikasına uygun iş ve işlemleri yapar.
c) İnternet sitesi yayın ekibi yöneticisi; internet sitesi yayın ekibinin koordinasyonu, denetimi ve yayınlanacak içeriğin kontrolünü sağlar.
ç) İnternet sitesi yöneticisi okul internet sitesi ile ilgili teknik iş ve işlemleri yürütür.
d) Editör; içerik oluşturur, oluşturulan tüm içeriklerin niteliğini artırmak üzere; anlam bütünlüğü, hitap tutarlılığı, noktalama, imla ve yazım kurallarına uygunluğunu denetler, değerlendirir ve düzeltmeler yapar.
e) Danışman; oluşturulan tüm içeriklerin pedagojik açıdan uygunluğunu denetler.

Panel kullanım ve içerik yönetim politikası

MADDE 8 – (1) Kullanıcı Yönetimi: İnternet sitesi yayın ekibi yöneticisi, kurum MEBBİS kullanıcı adı ve şifresi ile panele giriş yaparak internet sitesi yayın ekibi kullanıcı hesaplarını oluşturur. İnternet sitesi yayın ekibinden ayrılan veya internet sitesi yayın ekibine katılan kişilerin kullanıcı hesapları internet sitesi yayın ekibi yöneticisi tarafından güncellenir.

(2) Panelde yer alan, kuruma ait temel bilgilerin veri girişi yapılır.

(3) Okul adı, okul türü veya kurum kodu değişikliklerinde istenirse mevcut internet sitesi üzerinde okul adı ve alan adını değiştirerek kullanılmaya devam edilir. Okulun sehven birden fazla internet sitesi oluşturulması durumunda; panelde yer alan ilgili menüden kullanılmayan internet sitesi silinir.

(4) İçerik; hedef kitleye yönelik güncel, zengin ve tutarlı olur.

(5) Okul internet sitelerinde yayınlanacak içerikler: internet sitesinin etkin ve verimli kullanımını sağlamak amacıyla okul tanıtımı, öğrencilerin çeşitli alanlardaki proje çalışmaları, kültürel, sanatsal ve sportif faaliyetleri, öğretmenlerin hazırladıkları özgün eğitim içerikleri, rehberlik çalışmaları ve benzeri içerikleri kapsar.

(6) Oluşturulan içerikler, internet sitesi ziyaretçilerinin kurum hakkında olumlu bir algıya sahip olmalarına ve güven duygusunun oluşmasına, hedef kitlenin aidiyetlerinin artmasına yardımcı olacak nitelikte olur.

(7) Haber kategorisindeki içerikler; ne, nerede, ne zaman, nasıl, niçin, kim (5N 1K) sorularına cevap verecek şekilde hazırlanır. Haberler, kurumla doğrudan ilgili ve kurumsal kimliğe zarar vermeyecek nitelikte olur.

(8) Başkanlık tarafından yapılacak duyuru ve uyarılar panelden takip edilerek ivedi şekilde uygulanır.

(9) Benzer içerikler tek başlık altında veya liste şeklinde yayınlanır, içerik tekrarı yapılmaz. Bakanlığımız tarafından yürütülen projeler (MEBBİS, E-okul, www.meb.gov.tr, EBA ve benzeri) ve farklı sitelerde yer alan içerikler kopyalanarak tekrar oluşturacak şekilde yayınlanmaz ancak okulu ve hedef kitleyi doğrudan ilgilendiren içerikler alıntı olarak belirtilip, link verilerek yayınlanır.

(10) İlan ve bildirim niteliğindeki içerikler duyurular bölümünde yayınlanır.

(11) Doküman niteliğindeki içerikler menü içerisinde gruplanarak yayınlanır.

(12) Bağlantılar menüsüne sık kullanılan ve göz önünde bulunması gereken içerikler eklenir.

(13) Kişisel verilerin korunması kapsamında; internet sitesinde kişiyi tam olarak belirlenebilir kılan (T.C. Kimlik No, anne-baba adı, iletişim ve ikametgâh bilgileri ve benzeri) bilgilerin yer aldığı listeler yayınlanmaz.

(14) Okul internet sitesinde yönetici, öğretmen, diğer personel ve öğrencilere ait görsellerin yayınlanabilmesi için ilgiliden muvafakatname alınır. Okul internet sitesinde kullanılacak her türlü görsel bu muvafakatname esas alınarak seçilir.

(15) Hakkında koruma kararı bulunan öğrencilere ait bilgi ve fotoğraflar hiçbir surette yayınlanmaz.

(16) İnternet sitesinde, öğrenciler için eğitici niteliği olmayan, pedagojik açıdan sakıncalı içerik, bağlantı ve medya (oyun, video, uygulama ve benzeri) yayınlanmaz.

(17) Okul /kurum internet sitelerinde reklam yayınlanmaz.

(18) 6698 Sayılı Kişisel Verilerin Korunması Kanunu kapsamında, yayınlanacak her türlü içerik telif hakları, fikri haklar, şeref ve haysiyetin korunması ve gizlilikle uyumlu olur. Bakanlığın herhangi bir politikasını, kuralını ya da düzenlemesini ihlal edemez. Mevzuatla belirlenen hususlara aykırı olmaz.

(19) Panel Yetkilisi,

a) Panelde yer alan bilgilere zarar vermez; işleyişi aksatma, yavaşlatma veya durdurma eylemlerinde bulunmaz, içeriğini yetkisiz olarak değiştirmez.

b) Kendi kullanıcı bilgilerini; kimseyle paylaşmaz; bu bilgileri başkasının kullanımına izin vermez.

c) Bilgi teknolojileri kapsamında, panelde yer alan herhangi bir kaynağı, hiç kimse adına ve yararına kullanmaz.

ç) Diğer panel yetkililerinin hesap bilgilerini kullanarak yetki gerektiren alanlara erişmez.

d) İnternet sitesinin çalışmasını etkileyen arızaları mümkün olan en kısa sürede uygun iletişim kanallarını kullanarak Başkanlığa rapor eder.

e) Panelde yer alan gizlilik gerektiren bilgileri, kişisel veriler ve veri içeren ekran görüntülerini paylaşmaz.

Teknik destek politikası

MADDE 9 – (1) İnternet sitesi ile ilgili teknik destek talepleri panel içerisindeki destek bölümünden iletilir.

(2) Teknik destek taleplerinde yazışma üslubu resmî yazışmalarda uygulanacak usul ve esaslar hakkında yönetmelik hükümlerine uygun olarak yapılır.

Güvenlik politikası

MADDE 10 – (1) Başkanlığın onayı olmadan Bakanlık sunucuları haricinde internet sitesi ve veri tabanı barındırılmaz.

(2) Herhangi bir siber saldırı halinde işlem yapılmadan, tespit edilen sorunlar Başkanlığa bildirilir.

(3) Tahsis edilen internet sitesi alanına virüs ve benzeri zararlı içerikler ile yetkisiz erişime neden olabilecek uygulamalar yüklenmez.

(4) İnternet sitesi barındırma alanı internet sitesi yayıncılığı dışında dosya depolama veya arşiv alanı olarak kullanılmaz.

Yürürlük

MADDE 11 – (1) Bu Yönerge onayı tarihinde yürürlüğe girer.

Yürütme

MADDE 12 – (1) Bu Yönerge hükümlerini Millî Eğitim Bakanı yürütür.

10.06.02

T.C.
MİLLÎ EĞİTİM BAKANLIĞI
Hukuk Hizmetleri Genel Müdürlüğü

Sayı : 14168703-10.06.02-E.2975829 07.03.2017
Konu : Okullarda Sosyal Medyanın Kullanılması

GENELGE
2017/12

İlgi : a) Türkiye Cumhuriyeti Anayasası
b) Birleşmiş Milletler Genel Kurulu tarafından kabul edilen 20/11/1989 tarihli Çocuk Haklarına Dair Sözleşmesi.
c) 1739 sayılı Milli Eğitim Temel Kanunu.
d) 5237 sayılı Türk Ceza Kanunu

Bakanlığımıza bağlı okul ve kurumlardaki yönetici, öğretmen ve öğrenciler tarafından okulda ders sırasında veya serbest zamanlarda yapılan faaliyet, eylem ve durumların görüntüsünün alındığı, sesinin kaydedildiği veya videosunun çekildiği; daha sonra bunların internet sitelerine yüklendiği veya sosyal medya ortamlarında paylaşıldığına ilişkin bilgiler Bakanlığımıza ulaşmaktadır.

İlgi (a) Türkiye Cumhuriyeti Anayasasının 20 nci maddesinde: "Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir. Bu hak; kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsar" ve 41 inci maddesinde: "Devlet, her türlü istismara ve şiddete karşı çocukları koruyucu tedbirleri alır." şeklinde,

İlgi (b) Çocuk Haklarına Dair Sözleşmenin 19 uncu maddesinde "Bu Sözleşme' ye taraf Devletler, çocuğun ana-babasının ya da onlardan yalnızca birinin, yasal vasi veya vasilerinin ya da bakımını üstlenen herhangi bir kişinin yanında iken ... her türlü istismar ve kötü muameleye karşı korunması için; yasal, idari, toplumsal, eğitsel bütün önlemleri alırlar." ve 29 uncu maddesinde "taraf devletler çocuk eğitiminin çocuğun kişiliğinin, yeteneklerinin, zihinsel ve bedensel yeteneklerinin mümkün olduğunca geliştirilmesi amacına yönelik olmasını kabul ederler." şeklinde,

İlgi (c) 1739 sayılı Milli Eğitim Temel Kanununun Genel Amaçlar başlıklı 2 nci maddesinin ikinci fıkrasında Türk Millî Eğitiminin Genel Amacı, "Türk Milletinin bütün fertlerini; Beden, zihin, ahlak, ruh ve duygu bakımlarından dengeli ve sağlıklı şekilde gelişmiş bir kişiliğe ve karaktere, hür ve bilimsel düşünme gücüne, geniş bir dünya görüşüne sahip, insan haklarına saygılı, kişilik ve teşebbüse değer veren, topluma karşı sorumluluk duyan; yapıcı, yaratıcı ve verimli kişiler olarak yetiştirmek." şeklinde hükümlere yer verilmiştir.

Ayrıca ilgi (d) 5237 sayılı Türk Ceza Kanunun 135 inci maddesinde: "Hukuka aykırı olarak kişisel verileri kaydeden kimseye altı aydan üç yıla kadar hapis cezası verilir.",

Adres: MEB Hukuk Hizmetleri Genel Müdürlüğü
Elektronik Ağ:
e-posta: zyildiz@meb.gov.tr

Ayrıntılı bilgi için: Zeynep YILDIZ HÖKELEKLİ
Milli Eğitim Uzman Yardımcısı
Tel: 03124134199

136 ncı maddesinde: "Kişisel verileri, hukuka aykırı olarak bir başkasına veren, yayan veya ele geçiren kişi, bir yıldan dört yıla kadar hapis cezası ile cezalandırılır.", 137 inci maddesinde: "(1) Yukarıdaki maddelerde tanımlanan suçların;

a) Kamu görevlisi tarafından ve görevinin verdiği yetki kötüye kullanılmak suretiyle,

b) Belli bir meslek ve sanatın sağladığı kolaylıktan yararlanmak suretiyle,

işlenmesi hâlinde verilecek ceza yarı oranında artırılır.", 138 inci maddesinde; "Kanunların belirlediği sürelerin geçmiş olmasına karşın verileri sistem içinde yok etmekle yükümlü olanlara görevlerini yerine getirmediklerinde altı aydan bir yıla kadar hapis cezası verilir" ve 138 inci maddesinde de "Kişisel verilerin kaydedilmesi, verileri hukuka aykırı olarak verme veya ele geçirme ve verileri yok etmeme hariç, bu bölümde yer alan suçların soruşturulması ve kovuşturulması şikâyete bağlıdır. " şeklinde düzenleme yapılmıştır.

Yukarıda zikredilen mevzuat hükümleri doğrultusunda il, ilçe, okul ve kurum yöneticileri tarafından, okul veya kurumlarında görev yapan tüm MEB personeli ile öğrenim gören öğrencilerin, kişilerle ilgili her türlü ses, yazı, görüntü ve video kayıtlarının internette veya farklı dijital ya da basılı ortamda hukuka aykırı şekilde paylaşılmasının Anayasaya, uluslararası sözleşmelere ve 1739 sayılı Kanununa aykırı olduğu; bu fiillerin Türk Ceza Kanununda suç olarak düzenlenmiş olduğu hususunda bilgilendirilmesi sağlanacak ve bu durumların önüne geçilmesi için gerekli önlemler alınacaktır.

Ayrıca, kişilerin psikolojik ve sosyal yönlerine olumsuz etki yapacak her türlü ses, görüntü ve video kayıtlarının genel ağ ortamlarına yüklediği ve paylaştığı tespit edilenler hakkında ilgili mevzuatı çerçevesinde gerekli yasal işlemler başlatılacak ve sonucundan Bakanlığa bilgi verilecektir.

Bilgilerinizi ve gereğini önemle rica ederim.

Yusuf TEKİN
Bakan a.
Müsteşar

DAĞITIM :
Gereği:
- A Planı
- B Planı

Adres: MEB Hukuk Hizmetleri Genel Müdürlüğü
Elektronik Ağ:
e-posta: zyildiz@meb.gov.tr

Ayrıntılı bilgi için: Zeynep YILDIZ HÖKELEKLİ
Milli Eğitim Uzman Yardımcısı
Tel: 03124134199

T.C.
MİLLÎ EĞİTİM BAKANLIĞI
Bilgi İşlem Grup Başkanlığı

Sayı : 49473396/703.03/861980 27/02/2014
Konu: İnternet ve Bilgi Güvenliği.

İlgi: a) 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun,
b) 11.04.2012 tarihli ve 565 sayılı Millî Eğitim Bakanlığı Bilgi ve Sistem Güvenliği Yönergesi.

Bakanlık olarak, 5651 sayılı Kanun gereği, bilgi güvenliği kapsamında, sistem ve kullanıcı bazlı güncel politikalar uygulanmaktadır. Bilginin gizlilik, erişilebilirlik ve bütünlük özelliklerini muhafaza etmeye, bilginin geçtiği yerlerin nasıl sınıflandırılacağına ve nasıl koruma altına alacağına dair çözümler oluşturulmaktadır.

Temel amaçlarımızdan biri, hizmet verdiğimiz tüm kesimler için, güvenli ve kesintisiz ağ hizmetini sağlamaktır. Bu amaçla; gerçekleşmesi olası tehditlere karşı, iç ağdaki trafiği ve internet trafiğini sağlıklı yönetebilmek için güvenlik duvarı, saldırı tespit ve koruma sistemleri, içerik filtreleme, spam analizi, antivirus vb. ürün ve uygulamaları kullanılmaktadır.

11 Nisan 2012 tarihinde Bilgi ve Sistem Güvenliği Yönergesi çıkarılmıştır. Bu yönerge ile kurum çalışanlarımıza, sistem ve bilgi güvenliği kapsamında, uyulması gereken kurallar, olması ve olmaması gereken tasarruflar açıklanmıştır. Buna rağmen gerek Bakanlık personelimizin bir kısmı, gerekse kurum dışından kişiler, uygulanan çözümleri aşmaya yönelik tutumlarda bulunmaktadırlar. Bu amaçla, bilgi ve sistem güvenliği anlamında kurum politikalarını hiçe sayma, uygulanan filtreleme çözümlerini delme, gereksiz yüksek trafik oluşturma, güvensiz yazılım kullanma vb. gibi durumlar tesbit edilmektedir. İlgi yönergenin 11. maddesinin 4. bendinde belirtildiği gibi "Telif hakları ve lisansları ihlal eden, Bakanlık ağında yoğun ağ trafiğine sebep olan, iki veya daha fazla kullanıcı arasında veri paylaşmak için kullanılan noktadan noktaya (Peer-to-peer - P2P) uygulamalar kullanılamaz. Dosya paylaşımı, anlık mesajlaşma programları ve yoğun ağ trafiğine sebep olan uygulamalar gerekli görüldüğünde Bakanlık tarafından filtrelenir." denilmektedir. Bu sebeple Bakanlık hattını kullanan kullanıcıların uygulanan güvenlik politika ve kuralları çerçevesinde davranmaları gerekmektedir.

Bakanlığımız olarak TTVPN Metro İnternet Projesinin hayata geçirilmesi ile birlikte İl Millî Eğitim Müdürlüklerimizde yer alan ADSL, VDSL gibi bağlantıların iptal edilerek Bakanlık hattı haricinde herhangi bir hat(ADSL, 3G, wireless vb.) kullanılması yasaklanmıştır. Ancak İl Millî Eğitim Müdürlüklerimiz bünyesinde kurum, şahsi veya benzeri yöntemlerle ADSL, VDSL, 3G, wireless gibi bağlantıların yapıldığı tespit edilmiştir. İlgi yönergenin 11. Maddesinin 6.bendinde "Kurum ağına sistem yöneticisinin bilgisi dışında herhangi bir aktif ağ cihazı eklenemez." denilmektedir.

Atatürk Blv. 06648 Kızılay/ANKARA
Elektronik Ağ http://bigb.meb.gov.tr
e-posta: bigb@meb.gov.tr

Ayrıntılı bilgi için: M. KARADAĞ - Şb. Müd.
Tel: (0 312) 413 11 82
Faks: (0 312) 417 50 09

Bu sebeple İl Millî Eğitim Müdürlüğü bünyesinde yer alan Bakanlık hattı haricindeki tüm internet hatlarının (ADSL, VDSL 3G, Wireless vb.) acilen iptal edilmesi, gelecekte Bakanlığın ilgili birimlerinin bilgisi olmadan bu ve benzeri bağlantılara izin verilmemesi ile belirtilen bağlantıları iptal ettirmeme konusunda ısrarcı davranış sergileyen personel veya kurum hakkında gerekli yasal süreç başlatılması gerekmektedir.

Oluşması muhtemel bilişim suçlarının önüne geçebilmek amacıyla yukarıda belirtilen çalışmaların acilen tamamlanarak, birimlerinizde çalışan personelin, sözü edilen ilgili Kanun ve Yönerge doğrultusunda tekrar bilgilendirilmesi hususunda;

Bilgilerinizi ve gereğini rica ederim.

Yusuf TEKİN
Bakan a.
Müsteşar

DAĞITIM:
B Planı.

Atatürk Blv. 06648 Kızılay/ANKARA
Elektronik Ağ:http://bigb.meb.gov.tr
e-posta: bigb@meb.gov.tr

Ayrıntılı bilgi için: M. KARADAĞ - Şb. Müd.
Tel : (0 312) 413 11 82
Faks: (0 312) 417 50 09

T.C.
MİLLÎ EĞİTİM BAKANLIĞI
Hukuk Hizmetleri Genel Müdürlüğü

Sayı : 14168703-10.06.02-E.2975829 07.03.2017
Konu : Okullarda Sosyal Medyanın
Kullanılması

GENELGE
2017/12

İlgi : a) Türkiye Cumhuriyeti Anayasası
b) Birleşmiş Milletler Genel Kurulu tarafından kabul edilen 20/11/1989 tarihli Çocuk Haklarına Dair Sözleşmesi.
c) 1739 sayılı Milli Eğitim Temel Kanunu.
d) 5237 sayılı Türk Ceza Kanunu

Bakanlığımıza bağlı okul ve kurumlardaki yönetici, öğretmen ve öğrenciler tarafından okulda ders sırasında veya serbest zamanlarda yapılan faaliyet, eylem ve durumların görüntüsünün alındığı, sesinin kaydedildiği veya videosunun çekildiği; daha sonra bunların internet sitelerine yüklendiği veya sosyal medya ortamlarında paylaşıldığına ilişkin bilgiler Bakanlığımıza ulaşmaktadır.

İlgi (a) Türkiye Cumhuriyeti Anayasasının 20 nci maddesinde: "Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir. Bu hak; kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsar" ve 41 inci maddesinde: "Devlet, her türlü istismara ve şiddete karşı çocukları koruyucu tedbirleri alır." şeklinde,

İlgi (b) Çocuk Haklarına Dair Sözleşmenin 19 uncu maddesinde "Bu Sözleşme' ye tarafDevletler, çocuğun ana–babasının ya da onlardan yalnızca birinin, yasal vasi veya vasilerinin ya da bakımını üstlenen herhangi bir kişinin yanında iken … her türlü istismar ve kötü muameleye karşı korunması için; yasal, idari, toplumsal, eğitsel bütün önlemleri alırlar." ve 29 uncumaddesinde "taraf devletler çocuk eğitiminin çocuğun kişiliğinin, yeteneklerinin, zihinsel ve bedensel yeteneklerinin mümkün olduğunca geliştirilmesi amacına yönelik olmasını kabul ederler." şeklinde,

İlgi (c) 1739 sayılı Milli Eğitim Temel Kanununun Genel Amaçlar başlıklı 2 nci maddesinin ikinci fıkrasında Türk Millî Eğitiminin Genel Amacı, "Türk Milletinin bütün fertlerini; Beden, zihin, ahlak, ruh ve duygu bakımlarından dengeli ve sağlıklı şekilde gelişmiş bir kişiliğe ve karaktere, hür ve bilimsel düşünme gücüne, geniş bir dünya görüşüne sahip, insan haklarına saygılı, kişilik ve teşebbüse değer veren, topluma karşı sorumluluk duyan; yapıcı, yaratıcı ve verimli kişiler olarak yetiştirmek." şeklinde hükümlere yer verilmiştir.

Ayrıca ilgi (d) 5237 sayılı Türk Ceza Kanunun 135 inci maddesinde: "Hukuka aykırı olarak kişisel verileri kaydeden kimseye altı aydan üç yıla kadar hapis cezası verilir.",

136 ncı maddesinde: "Kişisel verileri, hukuka aykırı olarak bir başkasına veren, yayan veya ele geçiren kişi, bir yıldan dört yıla kadar hapis cezası ile cezalandırılır.", 137 inci

Adres: MEB Hukuk Hizmetleri Genel Müdürlüğü
Elektronik Ağ:
e-posta: zyildiz@meb.gov.tr
Ayrıntılı bilgi için: Zeynep YILDIZ HÖKELEKLİ
Milli Eğitim Uzman Yardımcısı
Tel: 03124134199

maddesinde: “(1) Yukarıdaki maddelerde tanımlanan suçların;

a) Kamu görevlisi tarafından ve görevinin verdiği yetki kötüye kullanılmak suretiyle,

b) Belli bir meslek ve sanatın sağladığı kolaylıktan yararlanmak suretiyle,

işlenmesi hâlinde verilecek ceza yarı oranında artırılır.”, 138 inci maddesinde: “Kanunların belirlediği sürelerin geçmiş olmasına karşın verileri sistem içinde yok etmekle yükümlü olanlara görevlerini yerine getirmediklerinde altı aydan bir yıla kadar hapis cezası verilir” ve 138 inci maddesinde de “Kişisel verilerin kaydedilmesi, verileri hukuka aykırı olarak verme veya ele geçirme ve verileri yok etmeme hariç, bu bölümde yer alan suçların soruşturulması ve kovuşturulması şikâyete bağlıdır. ” şeklinde düzenlenme yapılmıştır.

Yukarıda zikredilen mevzuat hükümleri doğrultusunda il, ilçe, okul ve kurum yöneticileri tarafından, okul veya kurumlarında görev yapan tüm personel ile öğrenim gören öğrencilerin, kişilerle ilgili her türlü ses, yazı, görüntü ve video kayıtlarının internette veya farklı dijital ya da basılı ortamda hukuka aykırı şekilde paylaşılmasının Anayasaya, uluslararası sözleşmelere ve 1739 sayılı Kanununa aykırı olduğu; bu fiillerin Türk Ceza Kanununda suç olarak düzenlenmiş olduğu hususunda bilgilendirilmesi sağlanacak ve bu durumların önüne geçilmesi için gerekli önlemler alınacaktır.

Ayrıca, kişilerin psikolojik ve sosyal yönlerine olumsuz etki yapacak her türlü ses, görüntü ve video kayıtlarının genel ağ ortamlarına yüklediği ve paylaştığı tespit edilenler hakkında ilgili mevzuatı çerçevesinde gerekli yasal işlemler başlatılacak ve sonucundan Bakanlığa bilgi verilecektir.

Bilgilerinizi ve gereğini önemle rica ederim.

Yusuf TEKİN
Bakan a.
Müsteşar

DAĞITIM :
Gereği:
- A Planı
- B Planı

Adres: MEB Hukuk Hizmetleri Genel Müdürlüğü
Elektronik Ağ:
e-posta: zyildiz@meb.gov.tr

Ayrıntılı bilgi için: Zeynep YILDIZ HÖKELEKLİ
Milli Eğitim Uzman Yardımcısı
Tel: 03124134199

Erasmus+

eTwinning

KATILIM BELGESİ

Sayın Erol KESKİN

İnternet Güvenliği ve eTwinning Etiği kursunu
başarıyla tamamlayarak
bu sertifikayı almaya hak kazandınız

M. Fatih DOĞER
eTwinning Türkiye
Ulusal Destek Servisi Koordinatörü

M. Hakan BÜCÜK
Yenilik ve Eğitim Teknolojileri Genel Müdürlüğü
Daire Başkanı

Erasmus+

eTwinning

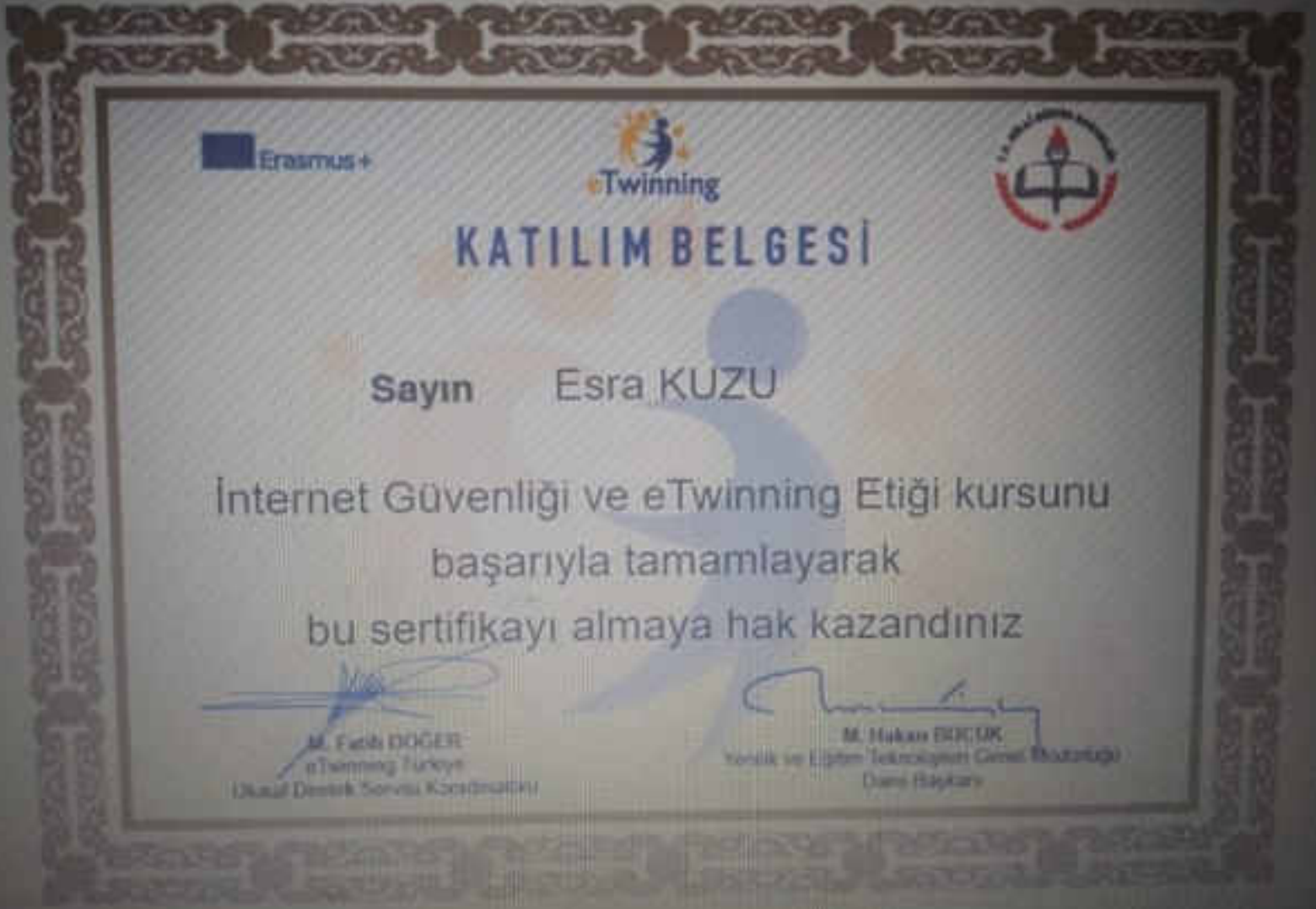
KATILIM BELGESİ

Sayın Hale Evircan Demir

İnternet Güvenliği ve eTwinning Etiği kursunu
başarıyla tamamlayarak
bu sertifikayı almaya hak kazandınız

M. Fatih DOĞER
eTwinning Türkiye
Ulusal Destek Servisi Koordinatörü

M. Hakan BÜCÜK
Yenilik ve Eğitim Teknolojileri Genel Müdürlüğü
Daire Başkanı


Erasmus+
eTwinning
KATILIM BELGESİ
Sayın Esra KUZU
İnternet Güvenliği ve eTwinning Etiği kursunu
başarıyla tamamlayarak
bu sertifikayı almaya hak kazandınız
M. Fatih DOĞER
eTwinning Türkiye
Ulusal Destek Servisi Koordinatörü
M. Hakan BİÇİK
Yenilik ve Eğitim Teknolojileri Genel Müdürlüğü
Daire Başkanı

Erasmus+

eTwinning

KATILIM BELGESİ

Sayın özlem evirgen

İnternet Güvenliği ve eTwinning Etiği kursunu
başarıyla tamamlayarak
bu sertifikayı almaya hak kazandınız

M. Fatih DOĞER
eTwinning Türkiye
Ulusal Destek Servisi Koordinatörü

M. Hakan BÜCÜK
Yenilik ve Eğitim Teknolojileri Genel Müdürlüğü
Daire Başkanı

Erasmus+

eTwinning

KATILIM BELGESİ

Sayın Sevilay Dinç

İnternet Güvenliği ve eTwinning Etiği kursunu
başarıyla tamamlayarak
bu sertifikayı almaya hak kazandınız

M. Fatih DOĞER
eTwinning Türkiye
Ulusal Destek Servisi Koordinatörü

M. Hakan BÜCÜK
Yenilik ve Eğitim Teknolojileri Genel Müdürlüğü
Daire Başkanı

Erasmus+

eTwinning

KATILIM BELGESİ

Sayın Betül ÇELEBİ UZGUR

İnternet Güvenliği ve eTwinning Etiği kursunu
başarıyla tamamlayarak
bu sertifikayı almaya hak kazandınız

M. Fatih DOĞER
eTwinning Türkiye
Ulusal Destek Servisi Koordinatörü

M. Hakan BÜCÜK
Yenilik ve Eğitim Teknolojileri Genel Müdürlüğü
Daire Başkanı

Erasmus+

eTwinning

KATILIM BELGESİ

Sayın Alev Karagoz

İnternet Güvenliği ve eTwinning Etiği kursunu
başarıyla tamamlayarak
bu sertifikayı almaya hak kazandınız

M. Fatih DOĞER
eTwinning Türkiye
Ulusal Destek Servisi Koordinatörü

M. Hakan BÜCÜK
Yenilik ve Eğitim Teknolojileri Genel Müdürlüğü
Daire Başkanı

Erasmus+

eTwinning

KATILIM BELGESİ

Sayın Deniz DAĞKIRAN

İnternet Güvenliği ve eTwinning Etiği kursunu
başarıyla tamamlayarak
bu sertifikayı almaya hak kazandınız

M. Fatih DÖĞER
eTwinning Türkiye
Ulusal Destek Servisi Koordinatörü

M. Hakan BÜCÜK
Yenilik ve Eğitim Teknolojileri Genel Müdürlüğü
Daire Başkanı

Erasmus+

eTwinning

KATILIM BELGESİ

Sayın Ebru AKGÜN

İnternet Güvenliği ve eTwinning Etiği kursunu
başarıyla tamamlayarak
bu sertifikayı almaya hak kazandınız

M. Fatih DOĞER
eTwinning Türkiye
Ulusal Destek Servisi Koordinatörü

M. Hakan BÜCÜK
Yenilik ve Eğitim Teknolojileri Genel Müdürlüğü
Daire Başkanı

Erasmus+

eTwinning

KATILIM BELGESİ

Sayın EŞREF ONUR

İnternet Güvenliği ve eTwinning Etiği kursunu
başarıyla tamamlayarak
bu sertifikayı almaya hak kazandınız

M. Fatih DOĞER
eTwinning Türkiye
Ulusal Destek Servisi Koordinatörü

M. Hakan BOCUK
Yenilik ve Eğitim Teknolojileri Genel Müdürlüğü
Daire Başkanı

Erasmus+

eTwinning

KATILIM BELGESİ

Sayın Filiz Alptekin

İnternet Güvenliği ve eTwinning Etiği kursunu
başarıyla tamamlayarak
bu sertifikayı almaya hak kazandınız

M. Fatih DOĞER
eTwinning Türkiye
Ulusal Destek Servisi Koordinatörü

M. Hakan BÜCÜK
Yenilik ve Eğitim Teknolojileri Genel Müdürlüğü
Daire Başkanı

Erasmus+

eTwinning

KATILIM BELGESİ

Sayın Filiz Şahin

İnternet Güvenliği ve eTwinning Etiği kursunu
başarıyla tamamlayarak
bu sertifikayı almaya hak kazandınız

M. Fatih DOĞER
eTwinning Türkiye
Ulusal Destek Servisi Koordinatörü

M. Hakan BÜCÜK
Yenilik ve Eğitim Teknolojileri Genel Müdürlüğü
Daire Başkanı

Erasmus+

eTwinning

KATILIM BELGESİ

Sayın Gönül Mutlu

İnternet Güvenliği ve eTwinning Etiği kursunu
başarıyla tamamlayarak
bu sertifikayı almaya hak kazandınız

M. Fatih DOĞER
eTwinning Türkiye
Ulusal Destek Servisi Koordinatörü

M. Hakan BÜCÜK
Yenilik ve Eğitim Teknolojileri Genel Müdürlüğü
Daire Başkanı

Erasmus+

eTwinning

KATILIM BELGESİ

Sayın HANDE ÇALIŞKAN

İnternet Güvenliği ve eTwinning Etiği kursunu
başarıyla tamamlayarak
bu sertifikayı almaya hak kazandınız

M. Fatih DOĞER
eTwinning Türkiye
Ulusal Destek Servisi Koordinatörü

M. Hakan BÜCÜK
Yenilik ve Eğitim Teknolojileri Genel Müdürlüğü
Daire Başkanı

Erasmus+

eTwinning

KATILIM BELGESİ

Sayın Kübra Ölmez

İnternet Güvenliği ve eTwinning Etiği kursunu
başarıyla tamamlayarak
bu sertifikayı almaya hak kazandınız

M. Fatih DOĞER
eTwinning Türkiye
Ulusal Destek Servisi Koordinatörü

M. Hakan BÜCÜK
Yenilik ve Eğitim Teknolojileri Genel Müdürlüğü
Daire Başkanı


Erasmus+
eTwinning
KATILIM BELGESİ
Sayın Mehmet AKALIN
İnternet Güvenliği ve eTwinning Etiği kursunu
başarıyla tamamlayarak
bu sertifikayı almaya hak kazandınız
M. Fatih DOĞER
eTwinning Türkiye
Ulusal Destek Servisi Koordinatörü
M. Hakan BUCUK
Yenilik ve Eğitim Teknolojileri Genel Müdürlüğü
Daire Başkanı

Erasmus+

eTwinning

KATILIM BELGESİ

Sayın nazlı mermer yılmaz

İnternet Güvenliği ve eTwinning Etiği kursunu
başarıyla tamamlayarak
bu sertifikayı almaya hak kazandınız

M. Fatih DOĞER
eTwinning Türkiye
Ulusal Destek Servisi Koordinatörü

M. Hakan BÜCÜK
Yenilik ve Eğitim Teknolojileri Genel Müdürlüğü
Daire Başkanı

Erasmus+

eTwinning

KATILIM BELGESİ

Sayın Orhan özkılınç

İnternet Güvenliği ve eTwinning Etiği kursunu
başarıyla tamamlayarak
bu sertifikayı almaya hak kazandınız

M. Fatih DOĞER
eTwinning Türkiye
Ulusal Destek Servisi Koordinatörü

M. Hakan BÜCÜK
Yenilik ve Eğitim Teknolojileri Genel Müdürlüğü
Daire Başkanı

Erasmus+

eTwinning

KATILIM BELGESİ

Sayın Özlem Dizili Demirci

İnternet Güvenliği ve eTwinning Etiği kursunu

başarıyla tamamlayarak

bu sertifikayı almaya hak kazandınız

M. Fatih DOĞER
eTwinning Türkiye
Ulusal Destek Servisi Koordinatörü

M. Hakan BÜCÜK
Yenilik ve Eğitim Teknolojileri Genel Müdürlüğü
Daire Başkanı

Erasmus+

eTwinning

KATILIM BELGESİ

Sayın Sevinç Ay Çalıkusu

İnternet Güvenliği ve eTwinning Etiği kursunu
başarıyla tamamlayarak
bu sertifikayı almaya hak kazandınız

M. Fatih DOĞER
eTwinning Türkiye
Ulusal Destek Servisi Koordinatörü

M. Hakan DEĞİRMENCİOĞLU
Yenilik ve Eğitim Teknolojileri Genel Müdürlüğü
Daire Başkanı

Erasmus+

eTwinning

KATILIM BELGESİ

Sayın Şerife Erdoğan

İnternet Güvenliği ve eTwinning Etiği kursunu
başarıyla tamamlayarak
bu sertifikayı almaya hak kazandınız

M. Fatih DÖĞER
eTwinning Türkiye
Ulusal Destek Servisi Koordinatörü

M. Hakan BÜCÜK
Yenilik ve Eğitim Teknolojileri Genel Müdürlüğü
Daire Başkanı

Erasmus+

eTwinning

KATILIM BELGESİ

Sayın Betül ÇELEBİ UZGUR

eSafety Label Hakkında Her Şey kursunu başarıyla tamamlayarak bu sertifikayı almaya hak kazandınız

M. Fatih DOĞER
eTwinning Türkiye
Ulusal Destek Servisi Koordinatörü

M. Hakan BÜCÜK
Yenilik ve Eğitim Teknolojileri Genel Müdürlüğü
Daire Başkanı

Erasmus+

eTwinning

KATILIM BELGESİ

Sayın Erol KESKİN

eSafety Label Hakkında Her Şey kursunu başarıyla tamamlayarak bu sertifikayı almaya hak kazandınız

M. Fatih DOĞER
eTwinning Türkiye
Ulusal Destek Servisi Koordinatörü

M. Hakan BÜCÜK
Yenilik ve Eğitim Teknolojileri Genel Müdürlüğü
Daire Başkanı

Erasmus+

eTwinning

KATILIM BELGESİ

Sayın Esra KUZU

eSafety Label Hakkında Her Şey kursunu başarıyla tamamlayarak bu sertifikayı almaya hak kazandınız

M. Fatih DOĞER
eTwinning Türkiye
Ulusal Destek Servisi Koordinatörü

M. Hakan BÜCÜK
Yenilik ve Eğitim Teknolojileri Genel Müdürlüğü
Daire Başkanı

Erasmus+

eTwinning

KATILIM BELGESİ

Sayın Nazlı MERMER YILMAZ

eSafety Label Hakkında Her Şey kursunu başarıyla tamamlayarak bu sertifikayı almaya hak kazandınız

M. Fatih DOĞER
eTwinning Türkiye
Ulusal Destek Servisi Koordinatörü

M. Hakan BÜCÜK
Yenilik ve Eğitim Teknolojileri Genel Müdürlüğü
Daire Başkanı

Erasmus+

eTwinning

KATILIM BELGESİ

Sayın Ozlem Dizili Demirci

eSafety Label Hakkında Her Şey kursunu başarıyla tamamlayarak bu sertifikayı almaya hak kazandınız

M. Fatih DOĞER
eTwinning Türkiye
Ulusal Destek Servisi Koordinatörü

M. Hakan BUCUK
Yenilik ve Eğitim Teknolojileri Genel Müdürlüğü
Daire Başkanı

Erasmus+

eTwinning

KATILIM BELGESİ

Sayın özlem evirgen

eSafety Label Hakkında Her Şey kursunu başarıyla tamamlayarak bu sertifikayı almaya hak kazandınız

M. Fatih DOĞER
eTwinning Türkiye
Ulusal Destek Servisi Koordinatörü

M. Hakan BÜCÜK
Yenilik ve Eğitim Teknolojileri Genel Müdürlüğü
Daire Başkanı

Erasmus+

eTwinning

KATILIM BELGESİ

Sayın Ali Y.K (Öğrenci)

İnternet Güvenliği ve eTwinning Etiği kursunu
başarıyla tamamlayarak
bu sertifikayı almaya hak kazandınız

M. Fatih DOĞER
eTwinning Türkiye
Ulusal Destek Servisi Koordinatörü

M. Hakan BÜCÜK
Yenilik ve Eğitim Teknolojileri Genel Müdürlüğü
Daire Başkanı

Erasmus+

eTwinning

KATILIM BELGESİ

Sayın Beren D. (Öğrenci)

İnternet Güvenliği ve eTwinning Etiği kursunu
başarıyla tamamlayarak
bu sertifikayı almaya hak kazandınız

M. Fatih DÖĞER
eTwinning Türkiye
Ulusal Destek Servisi Koordinatörü

M. Hakan BÜCÜK
Yenilik ve Eğitim Teknolojileri Genel Müdürlüğü
Daire Başkanı

Erasmus+

eTwinning

KATILIM BELGESİ

Sayın İlayda A.(Öğrenci)

İnternet Güvenliği ve eTwinning Etiği kursunu
başarıyla tamamlayarak
bu sertifikayı almaya hak kazandınız

M. Fatih DOĞER
eTwinning Türkiye
Ulusal Destek Servisi Koordinatörü

M. Hakan BÜCÜK
Yenilik ve Eğitim Teknolojileri Genel Müdürlüğü
Daire Başkanı

Erasmus+

eTwinning

KATILIM BELGESİ

Sayın D.Kibele D.(Öğrenci)

İnternet Güvenliği ve eTwinning Etiği kursunu
başarıyla tamamlayarak
bu sertifikayı almaya hak kazandınız

M. Fatih DÖĞER
eTwinning Türkiye
Ulusal Destek Servisi Koordinatörü

M. Hakan BÜCÜK
Yenilik ve Eğitim Teknolojileri Genel Müdürlüğü
Daire Başkanı

Erasmus+

eTwinning

KATILIM BELGESİ

Sayın Nida Ö. (Öğrenci)

İnternet Güvenliği ve eTwinning Etiği kursunu
başarıyla tamamlayarak
bu sertifikayı almaya hak kazandınız

M. Fatih DOĞER
eTwinning Türkiye
Ulusal Destek Servisi Koordinatörü

M. Hakan BÜCÜK
Yenilik ve Eğitim Teknolojileri Genel Müdürlüğü
Daire Başkanı

Checklist: Sexting

Are we doing this in our school?

	Yes	Partly	No
Policy			
1. Is sexting and our approach to it included in the child protection policy?	☑	☐	☐
2. Does the policy make reference to the role of the school in incidents which happen outside, i.e. when pupils are not at school?	☑	☐	☐
3. Are pupils aware of the consequences of sharing sexting-type images – both from school and law enforcement perspectives?	☑	☐	☐
4. Are the references to sexting regularly updated to reflect changes in the law and current practice and advice given to schools?	☑	☐	☐
Practice			
5. Do key staff receive regular training on the characteristics of sexting and the schools approach to it? Do they know how to respond to incidents?	☑	☐	☐
6. Do pupils receive information on how to deal with sexting, and how to seek further help and advice?	☑	☐	☐
7. Does our school employ strategies for engaging with parents on issues relating to sexting (e.g. information evenings, guidance on the school website)?	☑	☐	☐
8. Do we have systems in place to support parents who may encounter difficulties relating to sexting outside of school?	☑	☐	☐

Hale EVRİ
Okul Müdürü

Checklist: Schools on social networks

Are we doing this in our school?

	Yes	Partly	No
Policy			
1. School staff is kept informed about common policies concerning social media use, as well as possible restrictions.	☑	☐	☐
2. Pupils have been informed about the school's policies concerning social media use, as well as best practices, safe social media use and possible restrictions.	☑	☐	☐
Practice			
3. Staff sessions on social media use are held at least every six months.	☑	☐	☐
4. Parents are involved in and informed about social media practices.	☑	☐	☐
5. Pupils are involved in social media use at school. Pupils function as multipliers/ mentors to other pupils.	☑	☐	☐

Hale EVİRCAN
Okul Müdürü

Checklist: School policy

Are we doing this in our school?

	Yes	Partly	No
Infrastructure			
1. The school eSafety policy has up-to-date security systems including information about a firewall.	☑	☐	☐
2. All teachers receive CPD and regular training on eSafety and understand both the learning and administrative environments.	☑	☐	☐
3. One single person is responsible for licensing agreements ensuring they are up to date and fit for purpose (ICT or Network Manager).	☑	☐	☐
4. The eSafety policy gives clear guidelines on inappropriate and appropriate use of digital communications between stakeholders.	☑	☐	☐
Policy			
5. One single person is responsible for seeing that all aspects included in the school eSafety policy are discussed throughout the school and by all user groups (eSafety Coordinator).	☑	☐	☐

Hale EVİRCAN
Okul Müdürü

6. The school eSafety policy covers the following issues: use of digital and video images, data protection, unsuitable activities and copyright, mobile device use and illegal images.	☑	☐	☐

Practice

7. There is a clear and easy-to-access incident handling procedure in place.	☑	☐	☐
8. eSafety training for staff is delivered at least annually.	☑	☐	☐
9. All teachers receive CPD and regular training on eSafety (using the eSafety policy as a guide as to topics covered).	☑	☐	☐
10. The school eSafety policy refers to the integration of eSafety across the curriculum.	☑	☐	☐

Hale EVİRCAN
Okul Müdürü

Checklist: Safe passwords

Are we doing this in our school?

	Yes	Partly	No
Infrastructure			
1. Our ICT infrastructure is sufficiently secured; it automatically asks the users to renew their passwords to access the school system regularly.	☑	☐	☐
Policy			
2. The AUP contains information about passwords.	☑	☐	☐
3. Teachers periodically discuss with students the importance of effective, secure passwords.	☑	☐	☐
Practice			
4. Data protection is discussed as part of the curriculum.	☑	☐	☐

Hale EVİ[illegible]
Okul Müdürü

Checklist: Use of removable devices

Are we doing this in our school?

	Yes	Partly	No
Infrastructure			
1. Anti-virus protection is installed and regularly updated.	☑	☐	☐
Policy			
2. Ground rules on the use of removable devices are included in our AUP.	☑	☐	☐
3. Staff should not save sensitive data on removable devices.	☑	☐	☐
4. Incident handling procedures have been set up, especially in case of the loss of a removable device containing sensitive information about pupils.	☑	☐	☐
Practice			
5. Staff and pupils are required to always run a virus scan when using removable devices on school machines.	☑	☐	☐
6. Staff and pupils are sufficiently informed/trained to carry out successful virus scans.	☑	☐	☐
7. Staff and pupils are aware of and follow formal incident handling procedures (e.g. for loss of device, malware infection)	☑	☐	☐

Hale EVİRGEN
Okul Müdürü

Checklist: Taking and publishing photos and videos at school

Are we doing this in our school?

	Yes	Partly	No
Infrastructure			
1. One staff member is responsible for checking that personal data is not published next to pupils' photos on the school website.	☑	☐	☐
Policy			
2. There is a clear photograph and image policy with concrete guidelines. All teachers, parents, pupils and the wider school community are informed and regularly reminded about the policy.	☑	☐	☐
Practice			
3. The school maintains a database where the policy and supporting documents (photo and video permission forms) can easily be found.	☑	☐	☐
4. All teachers know where to receive guidance in case of doubt.	☑	☐	☐
5. The whole school community, including pupils, have received training concerning photos and use of social media.	☑	☐	☐
6. A reminder with guidelines is sent around before special events at school.	☑	☐	☐

Hale EVİRCAN
Okul Müdürü

eSafety Label
for a safer school

Checklist: Protecting sensitive data in schools

Are we doing this in our school?

	Yes	Partly	No
Infrastructure			
1. There are separate online environments (systems) for administration and learning.	☑	☐	☐
2. Anti-virus protection is regularly updated.	☑	☐	☐
3. Professional support is sought for secure storage and encryption.	☑	☐	☐
Policy			
4. We have a rigorously applied protocol on downloading/sending/printing sensitive data.	☑	☐	☐
5. Password info is included in our AUP.	☑	☐	☐
6. Good contact with our national Data Protection Commissioner's Office[1].	☑	☐	☐
Practice			
7. Relevant training for our staff from specialised expert.	☑	☐	☐
8. At minimum, an annual meeting with staff on importance of data protection including social engineering risks[2].	☑	☐	☐
9. An incident handling procedure is in place.	☑	☐	☐

Hale EVİRGAN DEMİR
Okul Müdürü

[1] You can find the contact details for the Data Protection Commissioner's Office in your country here: http://ec.europa.eu/justice/data-protection/bodies/authorities/eu/index_en.htm.
[2] Social engineering sites refer to sites where the user is tricked into visiting a website or clicking on a link to open an attachment, which they should not.

European Schoolnet

eSafety Label
for a safer school

Checklist: Protecting your devices against malware

Are we doing this in our school?	Yes	Partly	No
Infrastructure			
1. Anti-virus protection and firewalls are installed on all school devices and are regularly updated.	☑	☐	☐
2. Unwanted websites and pop-ups are permanently blocked on all school machines.	☑	☐	☐
Policy			
3. The AUP contains a strict protocol on downloading files, checking mails and use of portable devices.	☑	☐	☐
Practice			
4. Relevant training is provided for our staff from a specialised expert.	☑	☐	☐
5. There's a dedicated person to deal with any breaches of security that may occur.	☑	☐	☐
6. An incident handling procedure is in place.	☑	☐	☐
7. Pupils are informed on how they can scan files for malware on school devices.	☑	☐	☐
8. Pupils are informed about why it is important that specific online content remains blocked on school machines.	☑	☐	☐

Hale EVRENCAN DEMİR
Okul Müdürü

Checklist: Pupil's use of online technology outside school

Are we doing this in our school?

	Yes	Partly	No
Policy			
1. Our AUP includes a statement on how online issues which have taken place outside of school are dealt with.	☑	☐	☐
2. In case of serious problems, teachers are obliged to inform parents and call on external professional help when necessary.	☑	☐	☐
Practice			
3. Parents and pupils are informed about the school's commitment in regards such issues.	☑	☐	☐
4. Awareness raising activities on online issues are organised at least once per year.	☑	☐	☐
5. Staff trainings on online safety are organised annually.	☑	☐	☐
6. We have an appointed teacher or councillor where pupils can go for help related to online issues.	☑	☐	☐

Hale EVİRGAN DEMİR
Okul Müdürü

Checklist: Using mobile phones in schools

Are we doing this in our school?

	Yes	Partly	No
Infrastructure			
1. Our Wi-Fi network is not accessible for mobile phones.	☑	☐	☐
2. Our Wi-Fi network can be accessed by pupils, but is different from the secure network for staff/core business.	☑	☐	☐
Policy			
3. The AUP contains a strict protocol on the use of mobile devices in school.	☑	☐	☐
4. The school policy contains clear guidelines on the possession, use of mobile devices in school and the consequences of a violation of the policy.	☑	☐	☐
Practice			
5. The use of mobile devices is constructively incorporated in the curriculum.	☑	☐	☐
6. Teachers, pupils and parents are thoroughly informed about the policy on the use of mobile devices on school grounds.	☑	☐	☐
7. A strict procedure is applied by staff to deal with violations of the policy on mobile devices and the confiscation of devices.	☑	☐	☐

Hale EVİRGAN DEMİR
Okul Müdürü

Checklist: Information for parents

Are we doing this in our school?

	Yes	Partly	No
Policy			
1. Parents are asked to take an active role in eSafety at the school and to reinforce key messages. This is outlined clearly through our home/school agreement.	☑	☐	☐
Practice			
2. Parent sessions on eSafety are held at least annually.	☑	☐	☐
3. eSafety messages are distributed to parents through a range of different mediums.	☑	☐	☐
4. Pupils are involved in delivering eSafety messages to their parents.	☑	☐	☐

Hale Ev...
Okul Müdür...

Checklist: Incident handling

Did the school staff handle the incident correctly?

	Action needed	All good	Comment
General – process related			
1. Does the school policy/staff handbook include an incident handling procedure that all staff are aware of? Are contact numbers for helplines, etc. included? With the knowledge of this incident, can the current procedure be improved?	☐	☑	The school policy /staff hadbook include an incident handling procedure that all staff are aware of and contact numbers are included.The current procedure can be improved with the knowledge of this incident
2. Did everybody know how to handle the incident? In cases where respective parties, e.g. parents, police, etc. should have been involved/notified, was this done in the right and timely manner?	☐	☑	Everybody know how to handle the incident .All things were done in the right and timely manner.
3. Would it have been possible to discover the incident earlier?	☐	☑	It may be possible to predict the event by looking at previous data and clues.

Okul Müdürü

eSafety Label
for a safer school

Incidents concerning inappropriate access

4. Is there are a responsible person named that regularly monitors our services?	☐	☑	There is a responsible person 'Betül Çelebi Uzgur' named that regularly monitors our services.
5. Does our school have all sensitive data stored on a separate server to which only authorised personnel has access to?	☐	☑	Our school has all sensitive data stored on a separate server to which only authorised personnel has access to.
6. Are we aware of new security holes as they become known and apply patches accordingly?	☐	☑	We are aware of new security holes as they become known and apply patches accordingly.
7. Is our staff aware of the importance of securing sensitive data with secure passwords?	☐	☑	Our staff is aware of the importance of securing s ensitive data with secure passwords.

Incidents concerning bullying

8. Is there a person of confidence that students could discuss the incident with?	☐	☑	There is a person of confidence that students could discuss the incident with 'Betül Çelebi Uzgur'
9. Do all staff, pupils and members of the wider school community respect and adhere to the AUP?	☐	☑	All staff, pupils and members of the wider school community respect and adhere to the AUP.
10. Is there a risk that the incident could be repeated by the person causing it or against the same victim? Is there a need for further remedial work or awareness raising?	☐	☑	There is always risk.Also there is always a need for further remedial work of awareness raising because techonological systems are in a rapid change everyday.

Hale EVİRCAN DEMİR
Okul Müdürü

European Schoolnet

eSafety Label
for a safer school

Checklist: Online extremism, radicalisation and hate speech

Are we doing this in our school?

	Yes	Partly	No
Policy			
1. Are the risks of online extremism and radicalisation referred to in the child protection policy?	☑	☐	☐
2. Does the policy make reference to the role of the school in incidents which happen outside, i.e. when pupils are not at school?	☑	☐	☐
3. Are pupils and staff aware of the school's approach to hate speech?	☑	☐	☐
4. Are the references to online extremism and radicalisation regularly updated to reflect changes in the law and current practice and advice given to schools?	☑	☐	☐
Practice			
5. Do all staff receive regular training on the risks of radicalisation, are they aware of what to look for and how to spot potential problems? Do they know what to do if they have concerns?	☑	☐	☐
6. Do pupils receive information on how to protect themselves from online extremism and radicalisation?	☑	☐	☐
7. Does our school employ strategies for engaging with parents on issues relating to online extremism and radicalisation (e.g. information evenings, guidance on the school website)?	☑	☐	☐
8. Do we have systems in place to support parents who may encounter difficulties relating to online extremism and radicalisation outside of school?	☑	☐	☐

Hale EVİRGAN DEMİR
Okul Müdürü

9. Are there opportunities to provide a counter-narrative to hate speech and online extremism throughout the curriculum?

☑ ☐ ☐

Hale EVİRGİN
Okul Müdürü

eSafety Label
for a safer school

Checklist: Embedding eSafety in the curriculum

Are we doing this in our school?

	Yes	Partly	No
Infrastructure			
1. While our ICT infrastructure is sufficiently secured and internet access is filtered, this does not restrict our pupils' ability to explore the many online opportunities.	☑	☐	☐
Policy			
2. School policies explicitly refer to the integration of eSafety across the curriculum, so that all teachers are made aware of their shared responsibility.	☑	☐	☐
Practice			
3. eSafety is taught as part of the curriculum.	☑	☐	☐
4. All teachers receive regular training on eSafety.	☑	☐	☐
5. Pupils do peer mentoring about eSafety.	☑	☐	☐
6. The school provides eSafety support for pupils outside of curriculum time.	☑	☐	☐

Hale FIDAN DEMİR
Okul Müdürü

European Schoolnet

eSafety Label
for a safer school

Checklist: eSafety training courses

Are we doing this in our school?

	Yes	Partly	No
Policy			
1. All staff are aware of and understand the AUP?	☑	☐	☐
2. Staff are updated on eSafety issues regularly, and at least annually.	☑	☐	☐
3. eSafety is part of staff induction for all new staff.	☑	☐	☐
Practice			
4. All staff have received some eSafety training during the last 12 months.	☑	☐	☐
5. There is a planned programme of eSafety training targeted at different groups of staff.	☑	☐	☐
6. The CPD is up to date and relevant and addresses current eSafety trends and issues.	☑	☐	☐
7. The eSafety training is provided by a recognised provider in the field of online safety.	☑	☐	☐

eSafety Label
for a safer school

Checklist: Cyberbullying

Are we doing this in our school?

	Yes	Partly	No
Infrastructure			
1. Does our school use network monitoring technology that flags up keywords or inappropriate language that may be associated with bullying? (Remember however, that such activity will typically take place outside of the school network and outside of the school day.)	☑	☐	☐
2. Does our school have a designated staff member (probably within the pupil care team/pastoral team) with responsibility for overseeing all bullying issues? (This person will be a contact point for reports and advice, will be able to recognise trends and will be responsible for regularly reviewing and amending all relevant policies.)	☑	☐	☐
3. Does our school provide a way for concerns regarding bullying to be reported anonymously?	☑	☐	☐
Policy			
4. Is there a whole-school anti-bullying policy?	☑	☐	☐
5. Does the policy include cyberbullying issues which may originate outside of school, and methods of responding to such incidents?	☑	☐	☐
6. Do we provide a classroom and school environment that supports positive behaviour and peer support?	☑	☐	☐
7. Is the whole school community (staff, pupils and parents) aware of the rules and consequences for bullying?	☑	☐	☐

European Schoolnet

8. Is the anti-bullying policy regularly reviewed and reinforced in order to see if adaptations are needed (e.g. in case of new technology or research findings)? ☑ ☐ ☐

Practice

9. Do all teaching and support staff receive regular training on the characteristics of online and offline bullying, and appropriate responses to it? ☑ ☐ ☐
10. Do pupils of all ages receive information on how to deal with cyberbullying, and how to seek further help and advice? ☑ ☐ ☐
11. Does our school employ strategies for engaging with parents on issues relating to bullying and cyberbullying (e.g. information evenings, guidance on the school website)? ☑ ☐ ☐
12. Do we have systems in place to support parents who may encounter difficulties relating to cyberbullying at home? ☑ ☐ ☐

Checklist: Acceptable Use Policy (AUP)

Are we doing this in our school?

	Yes	Partly	No
Infrastructure			
1. The school infrastructure takes account of new initiatives and ways of working such as Bring Your Own Device (BYOD) and the AUP is amended accordingly.	☑	☐	☐
Policy			
2. The school has an AUP which is regularly updated.	☑	☐	☐
3. The review of the AUP involves all stakeholders.	☑	☐	☐
Practice			
4. Staff regularly refer to the AUP with pupils to ensure that there is a shared understanding	☑	☐	☐
5. All staff, pupils and members of the wider school community respect and adhere to the AUP.	☑	☐	☐

Hale ŞVİRCAN DEMİR
Okul Müdürü

eSafety Label - Action Plan

Action plan submitted by Erol Keskin for ŞEHİT TEĞMEN SUBUTAY ALKAN ORTAOKULU - 27.12.2020 @ 21:32:25

By submitting your completed Assessment Form to the eSafety Label portal you have taken an important step towards analysing the status of eSafety in your school. Congratulations! Please read through your Action Plan carefully to see what you can do to improve eSafety further in your school. The Action Plan offers useful advice and comments, broken down into 3 key areas: infrastructure, policy and practice.

Infrastructure

Technical security

- Your school system is protected by a firewall. Ensure that the provision and management of the firewall are regularly reviewed and updated, as and when required.
- It is good practice that your ICT services are regularly reviewed, updated and removed if no longer in use.

Pupil and staff access to technology

- It is good that in your school computer labs can easily be booked. Consider the option of integrating other digital devices into the lessons as using them provides best practise for pupils in dealing with new media. Ensure that safety issues are also discussed.
- All staff and pupils are allowed to use USB memory sticks in your school. This is good practice, and your Acceptable Use Policy should stipulate that all removable media is checked before use in the school systems. Check the fact sheet on Use of removable devices at www.esafetylabel.eu/group/community/use-of-removable-devices to make sure you cover all security aspects.

Data protection

- It is good that your email system is protected and that you have a policy for the transfer of pupil data in place. In this regard, it is important to draw up guidelines so that all staff are clear about what to do if they discover inappropriate or illegal content on school machines. For further information see the fact sheet on Protecting sensitive data (www.esafetylabel.eu/group/community/protecting-sensitive-data-in-schools).
- There is a retention plan in place for your school detailing how specific school records are stored, archived and disposed. This is very good. Ensure that the plan is followed and review it regularly to ensure it relates to the Data Protection Act and other relevant legislation. Check the according fact sheet for more information.

Software licensing

- It is good that you can produce an overview of installed software and their licences in a short time frame with the

help of several people. Consider centralising this.

- It is important to ensure that all new staff are briefed about the effective processes you have for the installation of new software. This will mean that the security of your systems can be maintained and that staff can try out new software applications that will help teaching and learning.

IT Management

- It is good practice to ensure that the person in charge of the ICT network is fully informed of what software is on school-owned hardware and this should be clearly indicated in the School Policy and the Acceptable Use Policy. The person responsible for the network needs to be able to guarantee conformity with licensing requirements and that new software won't interfere with network operation.

- There is a mechanism set up in your school that allows any staff member to make a request for new hard/software - a request that leads to an informed decision within a reasonable amount of time. This is great as this way teacher can benefit from new technologies while still staying inline with school policy.

Policy

Acceptable Use Policy (AUP)

- In your school policy issues are regularly discussed. This is good practice as it ensures staff and pupils are aware of them. Do pupils and staff also have to sign related documents to confirm their awareness?

- It is good practise that whenever changes are put into place in your school, the school policies are revised if needed. Note though, that also changes outside the school can affect policies such as new legislations or changing technologies. Therefore please review your policies at least annually.

- It is excellent that eSafety is an integral part of several school policies. Do all staff make reference to it when appropriate through their teaching? Look for examples of good practice and share these with staff and pupils. Produce a short case study to highlight this good practice and upload it to your profile on the eSafety Label portal via your My school area as inspiration for other schools.

Reporting and Incident-Handling

- Please share the materials in which you tackle these issues especially with pupils and parents in the of the eSafety Label portal.

- It's good that you have a clear School Policy on handling out-of-school eSafety incidents; is the number of these declining? Start a discussion thread in the community on what other preventative measures or awareness raising activities could be used in order to reduce the number of issues further. Don't forget to anonymously document incidents on the Incident handling form (www.esafetylabel.eu/group/teacher/incident-handling), as this enables schools to share and learn from each other's strategies.

- Are all staff familiar with the procedure for dealing with material that could potentially be illegal? Is there a named person from the school senior leadership team who takes overall responsibility in this type of case? The procedure needs to be clearly communicated to all staff in the School Policy, and to staff and pupils in the

Acceptable Use Policy. Remember to report and suspected illegal content to your national INHOPE hotline (www.inhope.org).

- Ensure that all staff, including new members of staff, are aware of the guidelines concerning what to do if inappropriate or illegal material is discovered on a school machine. Ensure, too, that the policy is rigorously enforced. A member of the school's senior leadership team should monitor this.

Staff policy Pupil practice/behaviour

- When discussing eSafety pupils at your school can sometimes provide feedback on the activities . Involve them as much as possible so that the teacher recognises real life issues while the pupils are more engaged.

- Your school has a school wide approach of positive and negative consequences for pupil behaviour. This is good practice, please share your policy via the My school area of the eSafety portal so that other schools can learn from it.

School presence online

- Regularly check the content of the school's online presence on social media sites to ensure that there are no inappropriate comments. Set up a process for keeping the site/page up to date, and check the fact sheet on Schools on social networks (www.esafetylabel.eu/group/community/schools-on-social-networks) for further information to make sure that good practice guidelines have been followed. Get feedback from stakeholders about how useful the profile is.

Practice

Management of eSafety

- Technology develops rapidly. Consider sending the member of staff responsible for ICT to trainings and/or conferences regularly to keep them updated on new features and risks. Check out the Better Internet for Kids portal to stay up to date with the latest trends in the online world.

eSafety in the curriculum

- It is good practise that in your school Cyberbullying is discussed in the curriculum with pupils from a young age.

- It is excellent that consequences of online actions are discussed with pupils in all grades. Terms and conditions need to be read to fully understand contractual conditions. This can also concern aspects of data privacy. Another important topic is breach of copyright. Please share the materials used through the uploading evidence tool, accessible also via the My school area.

- Sexting is an issue which affects many young people. Sharing possible consequences and risks with them is important, as is the opportunity for some discussion around the issue. Sexting should be part of a broad and balanced eSafety curriculum.

- You may want to consider including sexting in your child protection policy to help to ensure a consistent whole-school approach to dealing with any incidents.

Extra curricular activities

- Consider carrying out a simple survey in order to establish what pupils are doing when they go online. This will help to inform eSafety education within the school. Share your survey questionnaire and results in the eSafety Label community via your My school area (avoiding publishing any personal information) so that other schools can benefit from your work and even share their results with you for comparative purposes.

Sources of support

- It is good to know that other school services are involved in eSafety issues (e.g. counsellors, psychologists, school nurse). Are they also invited to contribute to developing and regular review of your School Policy? Publish a case study about how this is managed in your school on your school profile page on the eSafety Label project website, so that others can learn from your experience.

- It is great that you have a staff member which is knowledgable in eSafety issues who acts as a teacher of confidence to pupils.

Staff training

- Your school makes sure that every teacher is trained on cyberbullying. Please share resources that are used in these trainings via uploading them to your My school area. Are you also monitoring the effect that this training had on the number of incidents?

- It should be a real benefit to your pupils that all staff receive regular training on eSafety issues. Continue to gather feedback from staff on the medium- and long-term benefits of the training and consult the eSafety Label portal to see suggestions for training courses at www.esafetylabel.eu/group/community/suggestions-for-online-training-courses.

The Assessment Form you submitted is generated from a large pool of questions. It is also useful for us to know if you are improving eSafety in areas not mentioned in the questionnaire. You can upload evidence of such changes via the Upload evidence on the My school area section of the eSafety Portal. Remember, the completion of the Assessment Form is just one part of the Accreditation Process, because the upload of evidence, your exchanges with others via the Forum, and your reporting of incidents on the template provided are all also taken into account.