İZMİR ÇİĞLİ İMKB MESLEKİ VE TEKNİK ANADOLU LİSESİ

İZMİR ÇİĞLİ İMKB VOCATIONAL AND TECHNICAL ANATOLIAN HIGH SCHOOL

KURUM E-GÜVENLİK POLİTİKASI

INSTITUTION E-SECURITY POLICY

İZMİR/ÇİĞLİ İMKB MESLEKİ VE TEKNİK ANADOLU LİSESİ

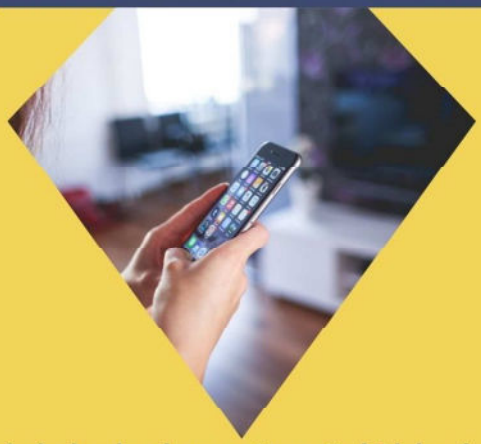
T.C ANAYASASINA / MİLLİ EĞİTİM BAKANLIĞI PROTOKOLLERİ / AVRUPA KOMİSYONU ESAFETY HAREKET EYLEM PLANINA / ÇOCUK HAKLARI BEYANNAMESİNE / AVRUPA İNSAN HAKLARI BEYANNAMESİNE GÖRE; E-GÜVENLİK İNTERNET GÜVENLİĞİ PROTOKOLLERİNİ UYGULAMAKTADIR.

Kurumumuzda izinsiz;

FOTOĞRAF ÇEKİLMEZ

KAMERA ÇEKİMİ YAPILMAZ

ÖĞRENCİLER CEP TELEFONU KULLANAMAZ



Bu kişinin hak ve özgürlüklerini ihlal eder.

Safer Internet Day

T.C MİLLİ EĞİTİM BAKANLIĞI

İZMİR/ÇİĞLİ

ÇİĞLİ İMKB MESLEKİ VE TEKNİK ANADOLU LİSESİ

E-GÜVENLİK POLİTİKASI VE AMAÇLARI

Teknolojinin hızla gelişmesiyle birlikte her okulun **Okul Güvenlik Politikası**'nın olma zorunluluğu doğmuştur. Paydaşlar okulumuzdan çeşitli şekillerde internete erişebilirler. Günlük hayatımızda hepimiz dijital teknolojilerle iç içe yaşar hale geldik. Öğrencilerimizin dijital teknolojileri en iyi nasıl kullanacaklarını bilmelerini sağlamak için, artık bunları nasıl kullanacaklarını bilmek ve anlamak gerekiyor. Bunun mümkün olan en güvenli şekilde ve en güvenli ortamda yapılmasını sağlamak için, öğrencilerimizin evde, okulda veya dışarıda ya da arkadaşlarıyla ya da yalnız olduğu zaman, dikkatini çeken açık ve özlü bir Güvenli İnternet Okul Politikasına sahip bir okuluz.

E-GÜVENLİK(E-SAFETY) POLİTİKAMIZ:

1) Okulumuzda ders anlatımı yapılan her alanda etkileşimli tahta ve Fatih internet erişim ağı vardır. Ders anlatımlarında EBA eğitim portalından sıklıkla yararlanılmaktadır. Fatih internet erişim ağı, ağ güvenlik filtresiyle kullanılmaktadır.
2) Okulumuzun internet sitesi vardır. Burada yayınlanan veriler kontrollü olarak paylaşılmaktadır.
3) Etkileşimli tahtalar güvenlik kurulumu ile Okul Fatih Projesi Koordinatörü, öğretmenler kontrolünde kullanılmaktadır.
4) Okulumuzda cep telefonları ders esnasında sınıfta cep telefonları için özel olarak yapılan kutuda ve kapalı konumda tutulmaktadır.
5) Rehberlik servisi ve bilişim alanı öğretmenleri tarafından, öğrencilerimize düzenli olarak, BİT bağımlılığı, BİT'nin doğru ve güvenli kullanımı, Siber Zorbalık gibi konularda seminerler tertiplenmektedir. Bu seminerler BİT uzmanları ve /veya emniyet görevlileri tarafından verilmektedir.
6) Okulumuzda BİT doğru ve güvenli kullanımı ile ilgili sabit panolar bulunmaktadır.
7) Okulumuzda etkileşimli tahtalar, fatih erişim ağı ve eba eğitim portalı kullanımının yoğun olması nedeniyle zümre öğretmenleri tarafından her zümrede BİT"nin doğru ve güvenli kullanımı, yapılan alıntıların derslere ve ödevlere aktarımı(kaynak kullanımı) ile ilgili kararlar alınmakta ve öğrenciler bu yönde bilgilendirilmektedir.
8) Okulumuzun öğretmenleri Milli Eğitim Bakanlığı tarafından verilen Siber Zorbalık, BİT'in doğru ve güvenli kullanımı konularında uzaktan ve yüz yüze eğitimler almıştır.
9) Okulumuzda "Daha Güvenli İnternet Günü" ile ilgili çalışmalar yapılmaktadır.
10) Okulumuzun internet sitesinde e-güvenlik konusunda, https://www.guvenliweb.org.tr/ sitesi ve buradan alıntılanan öğrenci ve velilere yönelik videolar ve afişler yer alan linkler yer almaktadır. Okul paydaşlarımız istedikleri zaman konu ile ilgili bilgi alabilmekteler.
11) Okulumuzda güvenli internet günü kutlamalarında, konu ile ilgili seminerlerde güvenliweb.org.tr. sitesinden alıntılanan bilgiler verilmektedir.
12) Rehberlik servisimiz internet etiği ve güvenli internet kullanımı konuları öğrencilerimize aktarılmaktadır.

13) Okulumuzda 21.yy iletişim becerileri önemsenmektedir. Bununla ilgili olarak öğrencilerimizin BİT kullanım becerilerini geliştirme çalışılmaları yapılmaktadır.
14) Okulumuzda Dijital vatandaş olma konusunda paydaşlarımızı bilinçlendirme çalışmaları yapılmaktadır.

E-GÜVENLİK POLİTİKASININ AMACI;

- Okulumuzun tüm üyelerini çevrimiçi olarak korumak ve güvenliğini sağlamak.
- Teknolojinin potansiyel riskleri ve yararları konusunda ÇİĞLİ İMKB MTAL idareci, öğretmeni, öğrenci ve çalışanları için farkındalık yaratmak.
- Tüm personelin güvenli ve sorumlu bir şekilde çalışmasını sağlamak, olumlu davranışları online olarak modellemek ve teknolojiyi kullanırken kendi standartlarını ve uygulamalarını yönetme gereksiniminin farkında olmak
- Okuldaki tüm üyeler tarafından bilinen çevrimiçi güvenlik endişelerine yanıt verirken açıkça kullanılacak prosedürleri tanımlamak.
- Bu politikanın, yönetim organı, öğretmenler, destek personeli, harici yükleniciler, ziyaretçiler, gönüllüler ve okul adına hizmet veren veya bunları yerine getiren diğer kişiler (toplu olarak bu politikada ´personel´ olarak anılacaktır) dahil olmak üzere tüm personel için geçerlidir) yanı sıra çocuklar ve ebeveynleri kapsamasını sağlamak,

Sonuç olarak hedefimiz, internet erişimi ve kişisel cihazlar da dahil olmak üzere bilgi iletişim cihazlarının kullanımı için bu güvenlik politikasının geçerli olmasıdır.; çocuklar, personel ya da diğer kişilere, çalıştıkları tüm cihazlar için geçerlidir.

KİLİT SORUMLULUKLARI ŞUNLARDIR:

- Çevrimiçi güvenlik politikalarının geliştirilmesine katkıda bulunmak.
- Kabul Edilebilir Kullanım Politikalarını okumak ve onlara bağlı kalmak.
- Okul sistemlerinin ve verilerin güvenliğinden sorumlu olmak.
- Çevrimiçi güvenlik konusundaki farkındalığa sahip olmak ve onların bakımında çocuklarla nasıl ilişkili olabileceklerini bilmek.
- Yeni ve gelişmekte olan teknolojiler kullanıldığında iyi uygulamaları modelleme o mümkün olduğunca müfredat ile çevrimiçi güvenlik eğitimini ilişkilendirmek.
- Okul koruma politikalarını ve prosedürlerini takip ederek endişe duyan bireylerin belirlenmesi ve uygun önlem alınmasını sağlamak.
- Olumlu öğrenme fırsatlarına vurgu yapmak. Bu alanda mesleki gelişim için kişisel sorumluluk almak.

ÖĞRENCİLERİN BAŞLICA SORUMLULUKLARI ŞUNLARDIR:

- Çevrimiçi güvenlik politikalarının geliştirilmesine katkıda bulunmak.
- Okulun Kabul Edilebilir Kullanım Politikalarını okumak ve onlara bağlı kalmak.
- Çevrimiçi ve çevrimdışı başkalarının hislerine ve haklarına saygı duymak.

❖ İhtiyaç halinde, güvenilir bir yetişkinden yardım istemek ve çevrimiçi güvenlik sorunlarıyla karşılaşan diğer kişileri desteklemek.

BİREYSEL; YAŞLARA, YETENEKLERE VE ZAYIF YÖNLERE UYGUN SEVİYELERDE:

❖ Kendilerini ve başkalarını çevrimiçi olarak korumak için sorumluluk almak.
❖ Yeni ve gelişmekte olan teknolojilerin getirdiği fırsatlar ile risklerle ilgili olarak kendinden sorumlu olmak.
❖ Teknolojiyi kullanmanın risklerini değerlendirmek ve bu riskler için sorumluluk sahibi davranmak.

EBEVEYNLERİN BAŞLICA SORUMLULUKLARI ŞUNLARDIR:

❖ 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.

ÇEVRİMİÇİ İLETİŞİM VE TEKNOLOJİNİN DAHA GÜVENLİ KULLANIMI

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 öğrencilerin izniyle ya da ebeveynlerinin izniyle yayınlanacaktır.
❖ Okul web sitesinin yönetici hesabı, yetkisi olmayan kişilerin girmesi engellenecektir.
❖ Okul, çevrimiçi güvenlik dahil olmak üzere, toplumun üyeleri için okul web sitesinde korunma hakkında bilgi gönderecektir.

Çevrimiçi Görüntü ve Videolar Yayınlama

❖ Okul, çevrimiçi paylaşılan tüm resimlerin ve videoların okul resim kullanımı politikasına uygun şekilde kullanılmasını sağlayacaktır.
❖ Okul , resimlerin ve videoların tümünün, veri güvenliği, Kabul Edilebilir Kullanım Politikaları, Davranış Kuralları, sosyal medya, kişisel cihazların ve cep telefonlarının kullanımı gibi diğer politikalar ve prosedürlere uygun şekilde yer almasını sağlayacaktır.
❖ Görüntü politikasına uygun olarak, öğrencilerin resimlerinin / videolarının elektronik olarak yayınlanmasından önce her zaman ebeveynlerin yazılı izni alınacaktır.

Video Konferans Kuralları

❖ Öğrenciler, bir video konferans araması veya mesajı hazırlamadan veya cevaplamadan önce bir öğretmenin iznini 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.

Kişisel Cihazların ve Cep Telefonlarının Kullanımı

❖ Cep telefonlarının ve çocukların, gençlerin ve yetişkinler arasındaki diğer kişisel cihazların yaygın bir şekilde sahiplenilmesi, tüm üyelerin cep telefonlarının ve kişisel cihazların sorumlu bir şekilde kullanılmasını sağlamak için gerekli adımları atmalarını gerektirir .
❖ Çocukların 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.
❖ 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.

Öğrencilerin Kişisel Cihazlarını ve Cep Telefonlarını Kullanımı

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

❖ Bilişim araçlarını, okul yönetimi ile öğretmenin bilgisi ve izni dışında konuşma yaparak, ses ve görüntü alarak, mesaj ve e-mail göndererek, bunları arkadaşlarıyla paylaşarak eğitim-öğretimi olumsuz yönde etkileyecek şekilde kullanmak aynı zamanda okul ders saatleri içerisinde telefon bulundurmak kesinlikle yasaktır.

❖ Öğrenciler ders başlamadan önce telefonlarını kapatmak ile yükümlüdür. Cep telefonunun amacı dışında kullanımı ihlali oluştuğunda, öğrenci, telefondaki özel verilerin korunmasını sağlamak amacıyla telefonunu kapatıp ders öğretmenine verir. Ders öğretmeni öğrenci telefonunu ilgili müdür yardımcısına teslim eder. Cep telefonu öğrenci velisine teslim edilinceye kadar güvenli bir yerde tutulur. Velisi dışında telefon kimseye teslim edilmez.

❖ Çocukların cep telefonlarının ve kişisel cihazların tüm kullanımları, kabul edilebilir kullanım politikasına uygun olarak gerçekleşecektir.

❖ Cep telefonları veya kişisel cihazlar, bir öğretmenin onayını alarak onaylanmış ve yönlendirilmiş müfredat tabanlı etkinlik kapsamında olmadıkları sürece dersler veya resmi okul saatlerinde öğrenciler tarafından kullanılamaz.

❖ Çocukların cep telefonlarını veya kişisel cihazlarını eğitim etkinliğinde kullanımı, okul idaresi tarafından onaylandığında gerçekleşecektir.

❖ Bir öğrenci ebeveynlerini arama gereği duyduğunda, okul idaresi tarafından temin edilen telefon kullanmasına izin verilecektir.

❖ Ebeveynlerin okul saatlerinde cep telefonuyla çocuklarıyla iletişim kurmamaları, okul idaresine başvurmaları önerilir. İstisnai durumlarda öğretmenin onayladığı şekilde istisnalara izin verilebilir.

❖ 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.

Ziyaretçiler Kişisel Cihazların ve Cep Telefonlarının Kullanılması

❖ Ebeveynler ve ziyaretçiler, okulun kabul edilebilir kullanım politikasına uygun olarak cep telefonlarını ve kişisel cihazları kullanmalıdır.

❖ Fotoğraflar veya videolar çekmek için ziyaretçiler ve ebeveynler tarafından cep telefonlarının veya kişisel cihazların kullanılması, okul resim kullanımı politikasına uygun olarak gerçekleştirilmelidir.

❖ Okul, ziyaretçilere kullanım beklentilerini bildirmek için uygun tabela ve bilgileri sağlayacak ve sunacaktır.

❖ Personelin uygun ve güvenli olduğunda sorunlara karşı çıkması beklenir ve her zaman ziyaretçilerin herhangi bir ihlalini idareye bildirecektir.

Çocukların ve Gençlerin Katılımı ve 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.
❖ 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.

Personelin Katılımı ve 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 Katılımı Ve Eğitimi

❖ ÇİĞLİ İMKB MTAL öğrencileri ,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.
❖ Okulumuzun bir parçası olarak ebeveynlerin çevrimiçi güvenlik bilgilerini okumaları istenecektir.
❖ Ebeveynler, Okula Kabul Edilebilir Kullanım Politikası´nı okumaya ve çocuklarıyla etkilerini tartışmaya teşvik edilecektir.
❖ Çevrimiçi güvenlik konusundaki ebeveynler için bilgi ve rehberlik, ebeveynlere çeşitli biçimlerde sunulacaktır.
❖ Ebeveynlerin, çevrimiçi olarak çocukları için olumlu davranışları rol modellemeleri teşvik edilecektir.

Çevrimiçi Olaylara ve Koruma Sorunlarına Yanıt Verme

❖ Okulun tüm üyeleri, sakıncalı mesajlaşma, 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, sakıncalı mesajlaşma, 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 o 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 yayımlamanın yasak olduğu bildirilecektir.
❖ 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.

(ENGLISH)

REPUBLIC OF TURKEY MINISTRY OF EDUCATION

İZMİR / ÇİĞLİ

ÇİĞLİ İMKB VOCATIONAL AND TECHNICAL ANATOLIAN HIGH SCHOOL

E-SAFETY POLICY AND OBJECTIVES

With the rapid development of technology, the obligation for every school to have a School Safety Policy has emerged. Stakeholders can access the internet from our school in various ways. In our daily life, we all have come to live with digital technologies. In order for our students to know how to best use digital technologies, it is now necessary to know and understand how to use them. To ensure this is done in the safest and safest way possible, we are a school with a clear and concise Safe Internet School Policy that draws the attention of our students when they are at home, at school or outside, or with friends or alone.

OUR E-SAFETY POLICY:

1) In our school, there are interactive boards and Fatih internet access network in every lecture area. EBA training portal is frequently used in lectures. Fatih internet access network is used with network security filter.

2) Our school has a website. The data published here are shared in a controlled manner.

3) Interactive boards are used under the control of the School Fatih Project Coordinator and teachers with security installation.

4) In our school, cell phones are kept in a box specially made for cell phones and in a closed position during the lessons.

5) The guidance service and informatics field teachers regularly organize seminars for our students on topics such as ICT addiction, correct and safe use of ICT, and Cyber Bullying. These seminars are given by ICT experts and / or law enforcement officials.

6) There are fixed boards in our school regarding the correct and safe use of ICT.

7) Due to the intensive use of interactive boards, fatih access network and eba education portal in our school, decisions are taken by the teachers in every class regarding the correct and safe use of ICT, the transfer of the quotations to the lessons and assignments (resource use) and the students are informed accordingly.

8) Teachers of our school have received remote and face-to-face trainings on Cyber Bullying, the correct and safe use of ICT given by the Ministry of National Education.

9) Studies on "Safer Internet Day" are carried out in our school.

10) Our school's website includes links on e-security, https://www.guvenliweb.org.tr/ and videos and posters for students and parents quoted here. Our school stakeholders can get information about the subject whenever they want.

11) Safeweb.org.tr at our school in safe internet day celebrations and seminars on the subject. The information quoted from the website is provided.

12) Our counseling service conveys internet ethics and safe internet usage issues to our students.

13) 21st century communication skills are important in our school. Related to this, studies are carried out to improve our students' ICT usage skills.

14) In our school, efforts are made to raise awareness of our stakeholders about being a digital citizen.

PURPOSE OF E-SAFETY POLICY;

- To protect and secure all members of our school online.
- Raising awareness for ÇİĞLİ İMKB MTAL administrators, teachers, students and employees about the potential risks and benefits of technology.
- To ensure that all personnel work safely and responsibly, to model positive behaviors online, and to be aware of the need to manage their own standards and practices while using technology
- Defining procedures to be used explicitly in responding to online safety concerns known to all members of the school.
- This policy applies to all staff, including the governing body, teachers, support staff, external contractors, visitors, volunteers, and others who serve or fulfill the school's behalf (collectively referred to as 'staff' in this policy) as well as to include children and parents,
- As a result, our goal is to have this security policy applicable to the use of information communication devices, including internet access and personal devices .; It applies to children, staff or other persons for all devices on which they work.

THE LOCK RESPONSIBILITIES ARE:

- Contributing to the development of online security policies.
- Reading and adhering to the Acceptable Use Policies.
- Being responsible for the security of school systems and data.
- To be aware of online safety and know how they may relate to children in their care.
- Modeling good practice when using new and emerging technologies. O Associating curriculum with online safety education as far as possible.
- Following school protection policies and procedures to identify individuals who are concerned and ensure that appropriate action is taken.
- Emphasizing positive learning opportunities. Taking personal responsibility for professional development in this field.

THE MAIN RESPONSIBILITIES OF STUDENTS ARE:

- ❖ Contributing to the development of online security policies.
- ❖ Read and adhere to the School's Acceptable Use Policies.
- ❖ Respecting the feelings and rights of others online and offline.
- ❖ If needed, seek assistance from a trusted adult and support others who encounter online security issues.

INDIVIDUAL; AT LEVELS SUITABLE FOR AGES, TALENTS AND WEAKNESSES:

- ❖ Taking responsibility for protecting themselves and others online.
- ❖ To be self-responsible for the opportunities and risks of new and emerging technologies.
- ❖ Evaluating the risks of using technology and acting responsibly for these risks.

THE MAIN RESPONSIBILITIES OF PARENTS ARE:

- ❖ Read the School Acceptable Use Policies, encourage their children to adhere to this policy, and ensure that they adhere to it as appropriate.
- ❖ Discussing online safety issues with their children, supporting the school's approaches to online safety and reinforcing appropriate safe online behaviors at home.
- ❖ Model the safe and appropriate use of technology and social media.
- ❖ Identifying changes in behavior that indicate that the child is at risk of harm online.
- ❖ Seek help or support from the school or other appropriate institutions if they or their children encounter problems or issues online.
- ❖ Contributing to the establishment of the school's online security policies.
- ❖ Using school systems such as learning platforms and other network resources in a safe and convenient way.
- ❖ To be responsible for their own awareness and learning of the opportunities and risks brought by new and emerging technologies.

SAFE USE OF ONLINE COMMUNICATION AND TECHNOLOGY

Managing the school / website:

- ❖ On the website, contact information will be school address, e-mail and telephone number. Personal information of staff or students will not be published.
- ❖ The School Principal will take overall publication responsibility for published online content and ensure that the information is accurate and appropriate.
- ❖ The website will comply with the school's publication guidelines, including accessibility, respect for intellectual property rights, privacy policies, and copyright.
- ❖ E-mail addresses will be carefully posted online to avoid spam mails.
- ❖ Student work will be published with the permission of the students or their parents.

❖ The administrator account of the school website will be blocked from unauthorized access.
❖ The school will post information about protection on the school website for members of the community, including online safety.

Publishing Images and Videos Online

❖ The school will ensure that all pictures and videos posted online are used in accordance with the school image use policy.
❖ The school will ensure that all images and videos are covered in accordance with data security, Acceptable Use Policies, Code of Conduct, social media, and other policies and procedures such as the use of personal devices and mobile phones
❖ In accordance with the image policy, written consent of the parents will always be sought before students' pictures / videos are published electronically.

Video Conference Rules

❖ Students will ask for permission from a teacher before they can prepare or reply to a video conference call or message.
❖ Videoconferencing will be supervised appropriately for the age and ability of the students.
❖ Parents' consent will be obtained before children participate in videoconferencing activities.
❖ Konferans Video conferencing will take place through formal and approved communication channels, following a robust risk assessment.
❖ Only main administrators will be granted access to video conference management areas or remote control pages.
❖ Private login and password information for educational video conferencing services will be given only to staff and will be kept confidential.

Use of Personal Devices and Cell Phones

❖ The widespread adoption of mobile phones and other personal devices among children, teens and adults requires all members to take steps to ensure responsible use of mobile phones and personal devices.
❖ The use of mobile phones and other personal devices by children and adults will be decided by the school and covered in appropriate policies, including the school Acceptable Use or Cell Phone Policy.
❖ Aware of the fact that personal communication with mobile technologies is an accepted part of daily life for children, staff and parents; however, it requires such technologies to be used safely and appropriately in school.

Students' Use of Personal Devices and Cell Phones

- Students will be trained in the safe and appropriate use of personal devices and mobile phones.
- It is strictly forbidden to use information tools in a way that adversely affects education and training by making speeches, taking sound and images, sending messages and e-mails, sharing them with friends without the knowledge and permission of the school administration and the teacher, and also having a telephone during school hours.
- Students are required to turn off their phones before the lesson starts. In case of a violation of the use of the mobile phone for purposes other than its intended purpose, the student turns off the phone and gives it to the lesson teacher in order to protect the private data on the phone. The course teacher delivers the student phone to the relevant deputy director. The mobile phone is kept in a safe place until it is handed over to the parent. The phone is not delivered to anyone except the parent.
- All use of children's mobile phones and personal devices will be carried out in accordance with the acceptable usage policy.
- Mobile phones or personal devices cannot be used by students in lessons or during official school hours unless they are part of an approved and directed curriculum-based activity with the consent of a teacher.
- Children's use of mobile phones or personal devices in the educational event will only take place when approved by the school administration.
- When a student needs to call their parents, they will be allowed to use a phone provided by the school administration.
- It is recommended that parents do not communicate with their children by mobile phones during school hours and contact the school administration. In exceptional cases, exceptions may be allowed as approved by the teacher.
- Students should only give their phone numbers to trusted friends and family members.
- Students will be taught the safe and appropriate use of mobile phones and personal devices, and the limits and consequences will be recognized.
- If it is suspected that material on a student's personal device or mobile phone may be illegal or may provide evidence of a criminal offense, the device is handed over to the police for further investigation.

Use of Personal Devices and Mobile Phones of Visitors

- Parents and visitors should use cell phones and personal devices in accordance with the school's acceptable use policy.
- The use of mobile phones or personal devices by visitors and parents to take photos or videos must be done in accordance with the school image use policy.
- The school will provide and present appropriate signage and information to inform visitors of their usage expectations.
- Staff are expected to confront problems when appropriate and safe, and will always report any violations of visitors to the administration.

Participation and Education of Children and Young People

❖ An online security (eSafety) curriculum is created to raise awareness among students about the importance of safe and responsible internet use and takes place throughout the school.
❖ Training on safe and responsible use will be done before internet access.
❖ Student contributions will be sought in writing and developing school online safety policies and practices, including curriculum development and implementation.
❖ Students will be supported to read and understand the Acceptable Use Policy in a manner appropriate to their age and abilities.
❖ All users will be notified that network and internet usage will be monitored. Acceptable Use prospects and Posters will be posted in all rooms with Internet access.
❖ Safe and responsible use of the internet and technology will be strengthened in the curriculum and in all subjects.
❖ Outside support will be used to complement and support schools' internal approaches to online security (eSafety) education.
❖ The school will reward students for their positive use of technology.
❖ The school will implement peer education to improve online safety in accordance with students' needs.

Participation and Training of Staff

❖ Online safety (eSafety) policy will be formally provided and discussed for the participation of all employees and strengthened and emphasized as part of our responsibility to protect.
❖ Staff will be aware that Internet traffic can be monitored and traced to a single user. Discretion and professional behavior are required when using school systems and devices.
❖ All members of staff will be provided with up-to-date and appropriate staff training on safe and responsible Internet use in a variety of ways on a regular (at least annual) basis, professionally and personally.
❖ All members of staff will realize that their online behavior can affect their role and reputation at school. Public, disciplinary or legal measures may be taken if something is thought to be found that puts the profession or institution in a state of corruption or has lost confidence in their professional abilities.
❖ Members of staff with responsibility for managing filtering systems or monitoring ICT usage will be overseen by the Leadership Team and have clear procedures for reporting issues or concerns
❖ The school highlights useful online tools that staff should use according to the age and abilities of the students.

Parental Participation and Education

❖ ÇİĞLİ İMKB MTAL students acknowledge that parents have an important role to play in order to become reliable and responsible users of the internet and digital technology.

❖ Parents' attention will be directed to school online safety (eSafety) policy and expectations on the school descriptions and school website.
❖ As part of our school, parents will be asked to read online safety information.
❖ Parents will be encouraged to read the School Acceptable Use Policy and discuss its effects with their children.
❖ Information and guidance for parents on online safety will be made available to parents in a variety of formats.
❖ Parents will be encouraged to role model positive behaviors for their children online.

Responding to Online Incidents and Protection Issues

❖ All members of the school, objectionable messaging, online / cyberbullying etc. You will be informed of the variety of online risks that can be encountered, including. This will be highlighted in staff training and educational approaches to students.
❖ All members of the school, filtering, objectionable messaging, cyberbullying, illegal content violation, etc. will be informed about the procedure for reporting online security (eSecurity) concerns such as.
❖ Digital Subscriber Line (DSL) will be notified of any online safety (e-Safety) incident involving child protection concerns, which will be recorded later.
❖ Complaints about misuse of the Internet will be handled within the school's complaints procedures.
❖ Online / cyberbullying complaints will be handled under the school's anti-bullying policy and procedure o Any complaints about staff misuse will be directed to the school principal
❖ School complaints procedure will be notified to students, parents and staff.
❖ Complaint and notification procedure will be notified to the staff.
❖ All members of the school should be aware of the importance of confidentiality and the need to follow formal school procedures to raise concerns.
❖ All members of the school will be reminded of safe and appropriate behavior online and notified that posting any content, comments, images or videos that constitute harm, distress, or a crime to any other member of the school community is prohibited.
❖ The school manages online safety (e-Security) incidents in accordance with the school discipline / behavior policy, when appropriate.
❖ The school notifies parents of concerns about these when needed.
❖ Once any investigation is complete, the school will receive information, identify lessons learned, and implement changes as necessary.
❖ Parents and children need to work together with the school to solve problems.