

**T.C.**

**NİLÜFER KAYMAKAMLIĞI**

**NİLÜFER İLÇE MİLLİ EĞİTİM MÜDÜRLÜĞÜ**

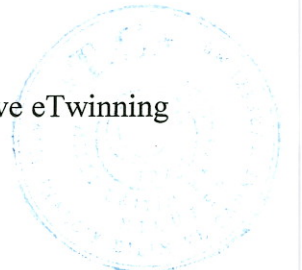
**HALİL İNALCIK BİLİM VE SANAT MERKEZİ**

**E-GÜVENLİK POLİTİKASI**



## **KABUL EDİLEBİLİR KULLANIM POLİTİKASI BİLGİLENDİRME METNİ**

- Kurumumuz, bilgisayarlar, tabletler ve cep telefonları gibi teknolojilerin aktif kullanıldığı dijital dünyadaki çocukların ve yetişkinlerin korunması için e-güvenliğin vazgeçilmez bir unsur olduğunun bilincindedir. Bu doğrultuda okulumuzda gerekli çalışmalar yapılmaktadır.
- Kurumumuz, sanal platformların ve bilgi iletişim teknolojilerinin günlük yaşamın önemli bir parçası olduğu inancıyla çocukların sanal ortamda karşılaştıkları riskleri yönetmeleri, bunlara tepki vermeleri ve stratejiler geliştirmenin yollarını öğrenmeleri için destekleyici çalışmalar yapmaktadır.
- Kurumumuz, eğitim standartlarını yükseltmek, başarıyı teşvik etmek, personelin mesleki çalışmalarını desteklemek ve yönetim işlevlerini geliştirmek için kurumda kaliteli internet erişimi sunma yükümlülüğüne sahiptir.
- Kurumumuz, tüm çocuklarımızın ve personelimizin sanal ortamlarda potansiyel tehlikelerden korunmasını sağlamaktan sorumludur.
- Kurumumuz atölyelerinde güvenli internet erişim ağı vardır. Güvenli internet erişim ağı, ağ güvenlik filtresiyle kullanılmaktadır.
- Kurumumuz internet sitesi yanında, facebook, twitter ve instagram hesapları bulunmaktadır. Bu ağların üzerinde yayınlanan veriler kontrollü olarak paylaşılmaktadır.
- Atölyelerde bulunan teknolojik aksam öğretmenlerin kontrolünde kullanılmaktadır.
- Kurumumuzda öğrencilerin izinsiz telefon kullanmaları yasaktır.
- Rehberlik servisi tarafından, öğrencilere yönelik, Bilinçli Teknoloji Kullanımı, siber zorbalık gibi konularda bilgilendirmeler yapılmakta ve seminerler düzenlenmektedir.
- Kurumumuzda Bilinçli Teknoloji Kullanımı ile ilgili sabit panolar bulunmaktadır.
- Kurumumuz öğretmenleri Milli Eğitim Bakanlığı tarafından verilen Siber Zorbalık, Bilinçli Teknoloji Kullanımı konularında uzaktan ve yüz yüze eğitimler almıştır/alacaktır.
- Kurumumuzda “Güvenli İnternet Günü” kutlanmaktadır.
- Kurumumuzun internet sitesinde e-güvenlik konusunda, [guvenliweb.org.tr](http://guvenliweb.org.tr) sitesi ve buradan alıntılanan öğrenci ve velilere yönelik videolar ve afişler yer alan linkler yer almaktadır.
- Kurum paydaşlarımız istedikleri zaman konu ile ilgili bilgi alabilmektedirler.
- Kurumumuzda güvenli internet günü kutlamalarında, konu ile ilgili seminerlerde [guvenliweb.org.tr](http://guvenliweb.org.tr) sitesinden alıntılanan bilgi broşürleri dağıtılmaktadır.
- Farklı atölyelerde; internet etiği ve güvenli internet kullanımı konularında öğrencilerimizle etkinlikler yapılmaktadır.
- Kurumumuzda 21.yy iletişim becerileri önemsenmektedir. Bununla ilgili olarak öğrencilerimizin Bilinçli Teknoloji Kullanım becerilerini geliştirme çalışmaları yapılmaktadır.
- Kurumumuzda Dijital vatandaş olma konusunda paydaşlarımızı bilinçlendirme çalışmaları yapılmaktadır.
- Kurumumuzda izinsiz fotoğraf çekmek kesinlikle yasaktır.
- Kurumumuz öğrencilerinin yüzleri okula ait hiçbir sosyal medya sitesinde ve eTwinning



portalı dahilindeki proje resimlerinde açık bir şekilde gösterilmeyecektir.

- Öğrencilerimizin ve velilerimizin kurumumuza kayıt olurken sağladıkları kişisel bilgileri idare sorumluluğunda ve tarafından korunmaktadır.
- Velilerimizin iletişim bilgileri kendi bilgi ve istekleri haricinde asla 3. şahıslarla paylaşılamaz.

## 1. AMAÇ

Bu e-Güvenlik politikasının amacı; Halil İnalçık Bilim ve Sanat Merkezi bilgisayar sistemlerinin ve iletişim teknolojilerinin kullanım koşullarını ve kabul edilebilir kullanım politikasını belirlemektir. Bu doğrultuda amaçlarımız:

- Kurumumuzun, bilişim teknolojileri ve internet etiğinin güvenli ve sorumlu kullanıldığı güvenilir bir ortam olduğundan emin olmak için toplumun tüm üyelerinden beklenen ana ilkeleri tanımlamak.
- Kurumumuz topluluğunun tüm üyelerini çevrimiçi olarak korumak ve güvenliğini sağlamak.
- Teknolojinin potansiyel riskleri ve yararları konusunda kurumumuz topluluğunun tüm üyelerinde 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.
- Kurumdaki tüm üyeler tarafından bilinen çevrimiçi güvenlik endişelerine yanıt verirken açıkça kullanılacak prosedürleri tanımlamak.
- Bu politikanın, yönetim organı, öğretmenler, öğrenciler, veliler, destek personeli, harici yükleniciler, ziyaretçiler, gönüllüler ve kurum adına hizmet veren veya bunları yerine getiren diğer kişiler (toplu olarak bu politikada 'personel' olarak anılacaktır) dahil olmak üzere tüm personel için geçerli olmasını sağlamak.

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

## 2. KAPSAM

Bu politika, Halil İnalçık Bilim ve Sanat Merkezi bilgisayar sistemlerine ve internet teknolojilerine kurum içinden veya dışından erişim hakkı verilen tüm kullanıcıları kapsar.

## 3. SORUMLULUKLAR

**Bu politikanın uygulanmasından idare sorumludur. Bu politikanın hazırlanmasından ve güncellenmesinden Halil İnalçık Bilim ve Sanat Merkezi idaresi ve e-Güvenlik Komisyonu sorumludur.**

### A. Tüm çalışanların kilit sorumlulukları şunlardır:

- ✓ Çevrimiçi güvenlik politikalarının geliştirilmesine katkıda bulunma.
- ✓ Kabul Edilebilir Kullanım Politikalarını (AUP'lar) okumak ve onlara bağlı kalmak.
- ✓ Kurum sistemlerinin ve verilerin güvenliğinden sorumlu olma.
- ✓ Bir dizi farklı çevrimiçi güvenlik konusundaki farkındalığa sahip olma ve onların bakımında çocuklarla nasıl ilişkili olabileceklerini bilme.
- ✓ Yeni ve gelişmekte olan teknolojiler kullanıldığında iyi uygulamaları modelleme.

- ✓ Mmkn olduėunca mfredat ile evrimii gvenlik eėitimini iliřkilendirme.
- ✓ Kurum koruma politikalarını ve prosedrlerini takip ederek endiře duyan bireyleri belirleme ve uygun nlem alma.
- ✓ Kiřisel teknoloji kullanımlarında, hem aık hem de kapalı alanda profesyonel bir davranıř seviyesinin korunması.
- ✓ Olumlu ėrenme fırsatlarına vurgu yapma.
- ✓ Bu alanda mesleki geliřim iin kiřisel sorumluluk alma.

#### **B. ocukların ve genlerin bařlıca sorumlulukları řunlardır:**

- ✓ evrimii gvenlik politikalarının geliřtirilmesine katkıda bulunmak.
- ✓ Kabul Edilebilir Kullanım Politikalarını (AUP'lar) okumak ve onlara baėlı kalmak.
- ✓ evrimii ve evrimdiřı bařkalarının hislerine ve haklarına sayėı duymak.
- ✓ İřler ters giderse, gvenilir bir yetiřkinden yardım istemek ve evrimii gvenlik sorunlarıyla karřılařan diėer kiřileri desteklemek.

#### **Bireysel yařlarına, yeteneklerine ve zayıf ynlerine uygun bir seviyede:**

- ✓ Kendilerini ve bařkalarını evrimii olarak korumak iin sorumluluk almak.
- ✓ Yeni ve geliřmekte olan teknolojilerin getirdiėi fırsatlar ve risklerle ilgili olarak kendi bilinci ve ėrenimlerinden sorumlu olmak.
- ✓ Belli bir teknolojiyi kullanmanın kiřisel risklerini deėerlendirmek ve bu riskleri sınırlamak iin gvenli ve sorumluluk sahibi davranmak.

#### **C. Ebeveynlerin bařlıca sorumlulukları řunlardır:**

- ✓ Kabul Edilebilir Kullanım Politikalarını (AUP'lar) okumak, ocuklarını bu politikaya baėlı kalmaya teřvik etmek ve uygun olduėunca kendilerinin de baėlı kalmasını saėlamak.
- ✓ ocuklarıyla evrimii gvenlik konularını tartıřmak, okulun evrimii gvenlik yaklařımlarını desteklemek ve evde uygun gvenli evrimii davranıřları pekiřtirmek.
- ✓ Teknoloji ve sosyal medyanın gvenli ve uygun kullanımını modellemek.
- ✓ Davranıřlarında, ocuėun evrimii olarak zarar grme tehlikesi altında olduėunu gsteren deėiřiklikleri belirlemek.
- ✓ Kurumumuzdan veya diėer uygun kurumlardan, kendileri veya ocukları evrimii problem veya sorunlarla karřılařırsa yardım veya destek istemek.
- ✓ Kurumun evrimii gvenlik politikalarının oluřturulmasına katkıda bulunmak.
- ✓ ėrenme platformları ve diėer aė kaynakları gibi kurum sistemlerini gvenli ve uygun bir Őekilde kullanmak.
- ✓ Yeni ve geliřmekte olan teknolojilerin getirdiėi fırsatlar ve risklerle ilgili olarak kendi bilinci ve ėrenimlerinden sorumlu olmak.

## **4. TANIMLAR**

### **Bilgisayar Sistemleri**

Her trl bilgisayar ile ilgili donanım, tehizat ve fikri mlkiyeti ifade eder. Buna, kurumumuzun sahip olduėu, kiraladıėı, uyarladıėı veya kurumumuzun sahipliėinde bulundurduėu, muhafaza altına aldıėı veya kontrol altında olan bilgisayar sistemleri, kiřisel bilgisayarlar, mobil cihazlar, bilgisayar aėları ve her trl yazılım, donanım yazılımı, iřletim yazılımı ve uygulama yazılımı dâhildir. Aık olmak adına, "bilgisayar sistemleri" kurumumuz tarafından uyarlanan yerel aė, bulut veya internet temelli hizmetleri veya kurumumuzun faaliyetlerinin veya kurum verisinin saklanması kullanılan genel nitelikli yerel aė, yrtlmesinde bulut veya internet temelli hizmetleri kapsar.



## 5. TEMEL PRENSİPLER

### Kullanım Koşulları

- ✓ Tüm kullanıcılar, Kurumun bilgisayar sistemlerini kullanarak:
  - Kurumun söz konusu sistemlerde saklanan veya bu sistemler aracılığıyla gönderilen hiçbir ileti veya verinin gizliliği hakkında herhangi bir beyanda bulunmadığını,
  - Kurumun bu dokümanda belirtilen haklarını saklı tuttuğunu,
  - Söz konusu sistemlerin kullanımının kurum onaylı amaçlar ile sınırlı olduğunu,
  - Bu hususta kendilerine gerekli bildirimlerin yapılmış olduğunu kabul ederler.
- ✓ Kurumun bilgisayar sistemlerinin kurum faaliyetleri ve önem arz etmeyen konulardaki kişisel kullanımı ile ilişkili olarak kullanılması bir hak değil ancak kurum topluluğunun sınırlı üyelerine tanınan bir ayrıcalıktır. Dolayısıyla, kurum dilediği zaman ve herhangi bir bildirimde bulunmaksızın bilgisayar sistemlerinin tamamına veya bir kısmına erişimi (tüm kullanıcılar veya bazı kullanıcılar için) tamamen veya kısmen engelleyebilir.
- ✓ Kurumun bilgisayar sistemleri kullanıcıları, işbu Halil İnalçık Bilim ve Sanat Merkezi Kabul Edilebilir Kullanım Politikası'na uymak zorundadırlar ve söz konusu sistemleri kullanarak, Kabul Edilebilir Kullanım Politikası'nı kabul ettiklerini ve ona uyacaklarını; Kabul Edilebilir Kullanım Politikası hakkında kendilerine bildirim yapılmış olduğunu; Kurumun Kabul Edilebilir Kullanım Politikası'nı uygulamasına izin verdiklerini kabul etmiş olurlar.
- ✓ Kullanıcılar aynı zamanda ilgili mevzuata uyacaklarını ve Kurum'u yükümlülük altına sokacak her türlü davranıştan kaçınacaklarını kabul ederler.
- ✓ Kurum, işbu Halil İnalçık Bilim ve Sanat Merkezi Kabul Edilebilir Kullanım Politikası ile bilgisayar sistemlerinin kullanımına ilişkin diğer koşulları dilediği zaman önceden herhangi bir bildirimde bulunmaksızın değiştirme hakkını ve ilgili mevzuat gereğince alınması gereken veya alınması uygun olan aksiyonları alma hakkını saklı tutar.
- ✓ Kurum, kurumun bilgisayar sistemleri ile kullanıcılarının tümünün söz konusu tesislerin yetkisiz veya uygunsuz kullanımına karşı korunması ve kurumun kural ve politikalarının ihlali veya ihlaline neden olacak muhtemel kullanımların tespiti için, herhangi bir bildirimde bulunmaksızın herhangi bir kişinin kullanımını sınırlama veya engelleme ve bilgisayar sistemleri için uygun görülen kullanımı zedeleyecek ya da kurumun kural veya politikalarının ihlali için kullanılabilecek olan her türlü veri, dosya veya sistem kaynağını araştırma, kopyalama, kaldırma veya değiştirme hakkını saklı tutar.
  - ✓ Halil İnalçık Bilim ve Sanat Merkezi bilgisayar sistemlerinin korunması için sistemlerin periyodik kontrolüne ilişkin hakları ve diğer her türlü hakkını saklı tutar. Kuruma ait bilgisayarlarda, akıllı tahtalarda, sunucularda, kurum sunucularında işlenen e-posta mesajlarında zararlı yazılım taraması sistemleri koruma amaçlı yapılacak kontrollere örnektir.
- ✓ Kurum, söz konusu sistemlerin gizlilik ve güvenliğinin sağlanması için gerçekleştireceği çalışmalardan, sistem bozukluğundan veya diğer bir sebepten meydana gelecek veri kaybından veya dosyalara müdahale edilmesinden sorumlu değildir.



## 6. ÇEVİRİMİÇİ İLETİŞİM VE TEKNOLOJİNİN DAHA GÜVENLİ KULLANIMI

### A. Kurum / Web Sitesinin Yönetilmesi

- Web sitesinde iletişim bilgileri kurum adresi, e-posta ve telefon numarası olacaktır. Personel veya öğrencilerin kişisel bilgileri yayınlanmayacaktır.
- Kurum 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 kurumun yayın yönergelerine uyacaktır.
- Spam maillerden korunmak için e-posta adresleri çevrimiçi olarak dikkatli bir şekilde yayınlanacaktır.
- Öğrenci çalışmaları öğrencilerin ve ebeveynlerinin izniyle yayınlanacaktır.
- Kurum web sitesinin yönetici hesabı, uygun bir şekilde güçlü şifreyle şifrelenerek korunacaktır.
- Kurum, çevrimiçi güvenlik dahil olmak üzere, toplumun üyeleri için okul web sitesinde korunma hakkında bilgi gönderecektir.

### B. Çevrimiçi Görüntü ve Videolar Yayınlama

- Kurum, çevrimiçi paylaşılan tüm resimlerin ve videoların kurum resim kullanımı politikasına uygun şekilde kullanılmasını sağlayacaktır.
- Kurum, 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.

### C. Kullanıcılar

- Öğrenciler, bir video konferans araması veya mesajı hazırlamadan veya cevaplamaadan önce bir öğretmeninden izin isteyecektir.
- Video konferans, öğrencilerin yaşı ve yeteneği için uygun bir şekilde denetlenecektir.
- 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 tutulacaktır.

### D. 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.

- Kurum, bir video konferansa katılmadan önce diğer konferans katılımcılarıyla diyalog kuracak. Kurum değilse, atölye için uygun olan materyali teslim aldığı kontrol edecektir.
- İnternetin ve ilgili cihazların uygun ve güvenli derslik kullanımı.
- İnternet kullanımı eğitimsel erişimin önemli bir özelliğidir ve tüm çocuklar bütünleşik bilsem müfredatının bir parçası olarak sorunlarını yanıtlamak için stratejiler geliştirmelerini destekleyecek ve onlara yardımcı olacak yaşa ve yeteneğe uygun eğitim alacaklardır.
- Kurumun internet erişimi eğitimi geliştirmek ve genişletmek için tasarlanacaktır.
- İnternet erişim seviyeleri müfredat gerekliliklerini 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.
- İçerik; Öğrencilerin yaşlarına ve yeteneklerine uygun olacaktır.
- Kuruma ait bütün cihazlar, kurumun Kabul Edilebilir Kullanım Politikasına uygun olarak ve uygun güvenlik önlemleri alınarak kullanılacaktır.
- Personel üyeleri, web sitelerini, araçlarını ve uygulamalarını atölyelerde kullanmadan önce veya evde kullanmayı önerirken daima değerlendirecektir.
- Öğrenciler, bilginin konumlanması, alınması ve değerlendirilmesi becerileri de dahil olmak üzere, internette araştırmada etkili kullanımı konusunda eğitilecektir.
- Kurum, personelin ve öğrencilerin internette türetilen materyallerin telif hakkı yasalarına uygun olmasını ve bilgi kaynaklarını kabul etmesini sağlayacaktır.
- Öğrencilere, okudukları veya gösterilen bilgilerin doğruluğunu kabul etmeden önce eleştirel düşünceleri öğretilenektir.
- Çevrimiçi materyallerin değerlendirilmesi, her konuda öğretme ve öğrenmenin bir parçasıdır ve müfredatta bir bütün olarak görülür.
- Kurum, öğrencileri ve çalışanlarımızın güvenli ve gizli bir ortamda iletişim kurmalarını ve işbirliği yapmalarını sağlamak için interneti kullanmaktadır.

#### **E. 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, gençlerin ve yetişkinlerin cep telefonlarının ve diğer kişisel cihazların kullanımı, kurum tarafından kararlaştırılacak ve kurum e-güvenlik veya Cep Telefonu Politikası dahil olmak üzere uygun politikalarda yer alacaktır.
- Kurumumuz, mobil teknolojilerle yapılan kişisel iletişimin, çocuklar, personel ve anne-babalar için gündelik yaşamın kabul edilen bir parçası olduğunun farkındadır; ancak, bu tür teknolojilerin kurumda güvenli ve uygun bir şekilde kullanılmasını gerektirir.



#### **F. Kişisel Cihazların ve Cep Telefonlarının Güvenli Bir Şekilde Kullanılması İçin Beklentiler**

- Kişisel cihazların ve cep telefonlarının kullanımı yasaya ve diğer uygun kurum politikalarına uygun olarak yerine getirilecektir.
- Sahaya getirilen her türlü elektronik cihazın sorumluluğu kullanıcıya aittir. Kurum, bu tür öğelerin kaybı, çalınması veya zarar görmesi konusunda sorumluluk kabul etmez.
- Kurum, 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.
- Kurumumuzun tüm üyelerine cep telefonlarını veya cihazlarını kayıp, hırsızlık veya hasardan korumak için adım atmaları önerilir.
- Kurumumuzun tüm üyelerinden, kayboldukları veya çalındığı takdirde yetkisiz aramaların veya hareketlerin telefonlarında veya cihazlarında yapılamayacağından emin olmak için şifreler / pim numaraları kullanmaları önerilir. Parolalar ve pin numaraları gizli tutulmalıdır. Cep telefonları ve kişisel cihazlar paylaşılmamalıdır.
- Kurumumuzun tüm üyelerine, cep telefonlarının ve kişisel cihazlarının saldırgan, küçümseyen veya başka şekilde kurum / ayar politikalarına aykırı düşen herhangi bir içerik içermediğinden emin olmaları önerilir.

#### **G. Öğrencilerin Kişisel Cihazlarını ve Cep Telefonlarını Kullanımı**

- Öğrenciler, kişisel cihazların ve cep telefonlarının güvenli ve uygun kullanımı konusunda eğitim alacaklardır.
- Bilişim araçlarını, kurum 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 kurum ders saatleri içerisinde telefon bulundurmak kesinlikle yasaktır.
- Çocukların cep telefonlarının ve kişisel cihazların tüm kullanımları, Kabul Edilebilir Kullanım Politikasına uygun olarak gerçekleşecektir.
- Cep telefonları veya kişisel cihazlar, öğrencilerin 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, kurum idaresi tarafından onaylandığında gerçekleşecektir.
- Bir öğrenci ebeveynlerini arama gereği duyduğunda, kurum telefonunu kullanmasına izin verilecektir.
- Ebeveynlerin kurum saatlerinde cep telefonu ile çocuklarıyla iletişim kurmamaları, kurum 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.

#### **H. 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 işte sağlanan ekipmanı kullanır.
- Personel herhangi bir kişisel cihazı doğrudan çocuklarla kullanmaz ve ders/eğitim etkinlikleri sırasında yalnızca kurum tarafından sağlanan ekipmanı kullanır.
- Personel, kişisel telefonların ve cihazların herhangi bir şekilde kullanımının daima veri koruma ve ilgili kurum 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 kurum 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 kurum 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 ulaşılabilecektir.
- Personelin cep telefonunu veya cihazlarını kişisel olarak kullanmalarını içeren herhangi bir iddiaya kurum yönetim politikasını izleyerek yanıt verilecektir.

#### **İ. Ziyaretçilerin Kişisel Cihazlarının ve Cep Telefonlarının Kullanılması**

- Ebeveynler ve ziyaretçiler, kurumun e-Güvenlik politikasına uygun olarak cep telefonlarını ve kişisel cihazları kullanmalıdır.
- Fotoğraflar veya videolar çekmek için ziyaretçiler ve ebeveynler tarafından cep telefonlarının veya kişisel cihazların kullanılması, kurum resim kullanımı politikasına uygun olarak gerçekleştirilmelidir.
- Kurum, 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.

## J. 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 kurumun tamamında yer alır.
- Güvenli ve sorumlu kullanım ile ilgili eğitim internet erişiminden önce yapılacaktır.
- Müfredat geliştirme ve uygulama da dahil olmak üzere kurum 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.
- Çevrimiçi güvenlik (e-Güvenlik) tüm derslere dahil edilecek ve hem güvenli kurum hem de evde kullanımını kapsayacaktır.
- Çevrimiçi güvenlik (e-Güvenlik) PSHE, SRE, Citizenship and Computing / BİT programlarına dahil edilecek ve hem güvenli kurum hem de evde kullanımını kapsayacaktır.
- E-Güvenlik beklentileri ve posterler, internet erişimi olan tüm odalarda yayınlanacaktır.
- İnternetin ve teknolojinin güvenli ve sorumlu kullanımı, müfredatta ve tüm konularda güçlenecektir.
- Dışarıdan destek, kurumların dahili çevrimiçi güvenlik (e-Güvenlik) eğitim yaklaşımlarını tamamlamak ve desteklemek için kullanılacaktır.
- Kurum, öğrencilerin teknolojiyi olumlu şekilde kullandıklarını ödüllendirecektir.
- Kurum, öğrencilerin ihtiyaçlarına uygun olarak çevrimiçi güvenliği geliştirmek için akran eğitimini uygulayacaktır.

## K. Personelin Katılımı ve Eğitimi

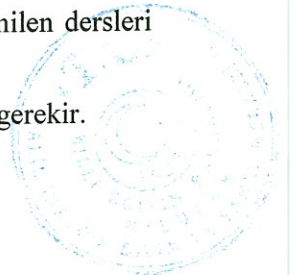
- Çevrimiçi güvenlik (e-Güvenlik) politikası, tüm çalışanların katılımı için resmi olarak sağlanacak ve tartışılacak ve korunma sorumluluğumuzun bir parçası olarak güçlendirilecek ve vurgulanacaktır.
- Personel, İnternet trafiğinin izlenebileceğini ve tek bir kullanıcıya kadar izlenebileceğinin farkında olacak. Kurum 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 kurumdaki 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.
- Kurum, çalışanların öğrencilerin yaşlarına ve yeteneklerine göre kullanması gereken yararlı çevrimiçi araçları vurgulamaktadır.

## **L. Ebeveynlerin Katılımı ve Eğitimi**

- Kurumumuz, çocukların internetin ve dijital teknolojinin güvenilir ve sorumlu kullanıcıları olabilmesi için ana-babaların oynayacakları önemli bir role sahip olduklarını kabul eder.
- Ebeveynlerin dikkatleri, kurum açıklamaları ve kurum web sitesinde kurum çevrimiçi güvenlik (e-Güvenlik) politikasına ve beklentilerine yönelecektir.
- Kurumlarımızın bir parçası olarak ebeveynlerin çevrimiçi güvenlik bilgilerini okumaları istenecektir.
- Ebeveynler, Kurum 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.

## **M. Çevrimiçi Olaylara ve Koruma Sorunlarına Yanıt Verme**

- Kurumun tüm üyeleri, cinsel içerikli mesajlaşma, çevrimiçi / siber zorbalık vb. dahil olmak üzere karşılaşılabilecek çevrimiçi risklerin çeşitliliğinden haberdar edilecektir. Bu, öğrencilere yönelik personel eğitimi ve eğitim yaklaşımları içerisinde vurgulanacaktır.
- Kurumun tüm üyeleri, filtreleme, cinsel içerikli 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 şikâyetler, kurumun şikâyet prosedürleri kapsamında ele alınacaktır.
- Çevrimiçi / siber zorbalık ile ilgili şikâyetler, kurumun zorbalık karşıtı politikası ve prosedürü kapsamında ele alınacaktır.
- Personelin yanlış kullanımı ile ilgili herhangi bir şikâyet kurum müdürüne yönlendirilecektir.
- Kurum şikâyet prosedürü öğrencilere, velilere ve personele bildirilecektir.
- Şikâyet ve ihbar prosedürü personele bildirilecektir.
- Kurumun tüm üyeleri, gizliliğin öneminden ve endişeleri bildirmek için resmi kurum usullerine uyma ihtiyacından haberdar olmalıdırlar.
- Kurumun tüm üyeleri, çevrimiçi ortamda güvenli ve uygun davranış hakkında hatırlatılacak ve kurum camiasının herhangi bir diğer üyesine zarar vermek, sıkıntı yaşamak veya suç oluşturan herhangi bir içerik, yorum, resim veya video yayımlamamanın önemini hatırlatacaktır.
- Kurum, çevrimiçi güvenlik (e-Güvenlik) olaylarını, uygun olduğunda, kurum disiplini / davranış politikasına uygun olarak yönetir.
- Kurum, ebeveynlere, ihtiyaç duyulduğunda bunlarla ilgili endişeleri bildirir.
- Herhangi bir soruşturma tamamlandıktan sonra kurum bilgi alacak, öğrenilen dersleri belirleyecek ve değişiklikleri gerektiği gibi uygulayacaktır.
- Sorunları çözmek için ebeveynlerin ve çocukların kurumla ortak çalışması gerekir.



## 7. YÖNTEM

### e-Güvenlik Politikası

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

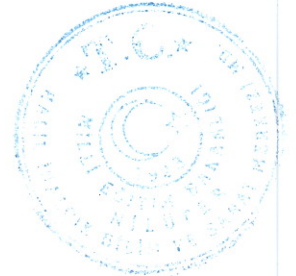
- Kurum, kuruma ait bilgisayar sistemleri üzerindeki tüm hak, mülkiyet ve çıkarlara sahiptir. Halil İnalçık Bilim ve Sanat Merkezi e-Güvenlik Politikası veya bilgisayar sistemlerinin kullanımına ilişkin olarak kurum tarafından herhangi bir mecrada yayımlanan hüküm ve koşullar altındaki hiçbir hüküm hiçbir şekilde söz konusu hak, mülkiyet ve çıkarların kullanıcılara devredildiği anlamına gelmemektedir. Kurum kullanıcılara sadece bilgisayar sistemlerinin kullanımına ilişkin şahsi, dünya genelinde, bedelsiz, devredilemeyen ve münhasır olmayan bir lisans tanımaktadır. Kullanıcılar bilgisayar sistemlerinin hiçbir yazılım veya diğer bir parçasını kopyalayamaz, değiştiremez, yeniden üretmez, bunlardan türemiş çalışma yaratamaz, tersine mühendislik yapamaz, parçalara ayıramaz veya diğer bir şekilde kaynak koduna dönüştüremez.
- Kullanıcılar, kurumun izin vermediği bilgisayar sistemlerini kullanamazlar. Bilgisayar sistemlerine erişebilmek için hatalı veya aldatıcı bilgilerin temin edilmesi suretiyle veya sair şekillerde bilgisayar sistemlerinin yetkisiz kullanımı yasaktır. Kullanıcılar diğer kurum, kuruluş veya kişilerin bilgisayar sistemlerine yetkisiz erişim sağlamak için okulun bilgisayar sistemlerini kullanamaz.
- Kullanıcılar, kurum hesaplarını kullanması için hiç kimseyi hiçbir sebeple yetkilendiremez. Kurum hesabının her türlü kullanımından hesap sahibi sorumludur. Kullanıcılar hesaplarının yetkisiz kişilerce kullanılmasının önüne geçilmesi için şifre koruma ve belge koruma dâhil tüm makul önlemleri almalıdır. Şifrelerini başka bir kişiyle paylaşmamalı ve şifrelerini düzenli olarak değiştirmelidir. Bir kullanıcı hesabına ait şifre kullanılarak gerçekleştirilen her türlü işlemde, söz konusu işlemi gerçekleştiren taraf hesap sahibinin kendisi olmasa dahi sorumlu hesap sahibidir.
- Kurumun bilgisayar sistemleri yalnızca izin verildiği şekilde kurum ile ilişkili hususlarda kullanılmalıdır. Tüm kurum donanımı için söz konusu olduğu üzere, kurum ağı dâhil bilgisayar sistemlerinin şahsi veya ticari amaçlar doğrultusunda kullanılması, açıkça izin verilmeyen haller dışında yasaktır. Kurumun bilgisayar sistemleri, hileli ya da hukuka aykırı bir şekilde elde edilmiş medya belgeleri ile yazılımların toplanması, yüklenmesi, dağıtılması dâhil ve bunlarla sınırlı olmamak üzere hiçbir hukuka aykırı amaç için kullanılamaz. Dış ağ veya hizmetlerin – bulut hizmetleri dâhil – kullanımı hem kurum hem de söz konusu ağ ve hizmetleri sunan kuruluşlar tarafından yayımlanan e-Güvenlik politikalarına uygun olmalıdır.
- Kullanıcılar kurumun ilgili personeli, bilgi güvenliği sorumlusu veya ilgili taraftan önceden izin almadıkça, herhangi bir bilgiye, kuruma ait yazılıma veya diğer belgelere (programlar, altyordam kitaplığı üyeleri, veri ve elektronik posta dâhil) erişemez; söz konusu bilgi, yazılım ve belgeleri değiştiremez, kopyalayamaz, taşıyamaz veya kaldıramaz. Kullanıcılar lisans verenden önceden izin almadıkça, üçüncü kişilere ait yazılımları kopyalayamaz, dağıtamaz, görüntüleyemez veya açıklayamaz. Kullanıcılar kullanımı için uygun bir şekilde lisanslanmamış olan yazılımları sistemlere yükleyemez.
- Kuruma ait hiçbir bilgisayar sistemi sorumsuz bir şekilde veya başkalarının işlerine

engel olacak şekilde kullanılamaz. Buna hakaret içerikli, rahatsız edici veya taciz edici içerikler; zincirleme mektup, yetkisiz toplu mail veya istenmeyen reklamların iletilmesi veya ulaşılabılır kılınması; kullanıcıya ait olmayan bir sistem, materyal veya bilgiye kasıtlı, dikkatsizce veya ihmalkâr bir biçimde zarar verilmesi; kasıtlı olarak elektronik iletişimin kesintiye uğratılması veya diğer bir şekilde başkalarının mahremiyetinin ihlal edilmesi veya kullanıcıya ait olmayan veya kullanıcı için olmayan bilgiye erişilmesi; sistem kaynaklarının kasıtlı olarak hatalı kullanılması veya başkalarının hatalı kullanmasının sağlanması veya ücretsiz yazılım gibi güvenilir olmayan kaynaklardan idari sistemlere yazılım veya veri indirilmesi dâhildir.

- Kurum, bilgisayar sistemlerine bizzat sağlamadığı içeriklerden hiçbir şekilde sorumlu değildir. Kullanıcılar başkaları tarafından verilen içeriklere, bunların hakaret içerici, uygunsuz veya sakıncalı olduğunu düşünebileceğini kabul ederek ve risk kullanıcının kendisine ait olmak üzere erişir. Bilgisayar sistemleri “OLDUĞU GİBİ” ve “MEVCUT HALİYLE” sunulmaktadır. Kurum, üçüncü taraf içeriklerinin doğru, tam ve güvenilir olduğuna ilişkin her türlü yükümlülükten kendini muaf tutmaktadır. Kullanıcı bilgisayar sistemlerinde bulundurduğu veya sakladığı bilgilerden kendisi sorumludur.
- Kullanıcı (i) bilgisayar sistemlerinin işleyişini veya söz konusu bilgisayar sistemlerinin başkaları tarafından kullanımını engelleyici her türlü harekete teşebbüsün; (ii) bilgisayar sistemlerine fazla yükleme yapacak içeriklerin yüklenmesinin; (iii) bilgisayar sistemlerinin genel güvenliğine tehlike arz edecek ve/veya diğer kullanıcıları zarara uğratacak hareketlerin; (iv) bilgisayar sistemlerinin işleyişini engelleyici veya müdahale edici yazılımların kullanılmasının veya kullanılmaya çalışılmasının mutlak bir biçimde yasak olduğunu kabul eder.
- İşbu politikanın başka bir kişi tarafından ihlaline veya bilgisayar sistemlerinin güvenliği ile ilgili bir hata ya da güvenliğin “by-pass” edilmesine ilişkin her türlü bilginin tespiti durumunda, vakanın Halil İnalçık Bilim ve Sanat Merkezi idaresine veya Kurum E-Güvenlik Komisyonu’na bildirilmesi zorunludur.
- Kurum bilgisayar sistemlerinin yetkisiz veya uygunsuz bir şekilde kullanımı, işbu politikaya uyulmaması dâhil, kurum politikasının ihlalini teşkil etmektedir ve İdare onayıyla Disiplin Kurulu takibini gerektirir. İşbu politikaya veya politikanın belli bir duruma uygulanmasına ilişkin her türlü soru kurum idaresine ya da E-Güvenlik Komisyonu’na iletilir.

## 8. GÖZDEN GEÇİRME

Bu dökümanı gözden geçirme ve güncelleştirme sorumluluğu kurum idaresine aittir. Yapılan değişiklik ve güncellemeler idare onayıyla yayınlanır. Gözden geçirme her yıl Haziran ayında yapılır.



**KURUM E-GÜVENLİK KOMİSYONU**



Serdar ERDEM

İngilizce Öğretmeni



Ömer ZENGİN

Uzman Psikolojik Danışman



İzzet UZUNARDALI

Bilişim Teknolojileri Öğretmeni



Hasibe ÖZER

Bilişim Teknolojileri Öğretmeni



Yüksel ÇEVİK

Müdür Yardımcısı



Erol ERTÜRK

Kurum Müdürü

