

# Hüseyin Polat Özel Eğitim Uygulama Okulu

## e-Güvenlik Politikası

### 1. Çevrimiçi Güvenlik Etik Kuralları Oluşturma

#### 1.1 Amaçlar ve politika kapsamı

##### 1.1 Olası beyanlar:

- Hüseyin Polat Özel Eğitim Uygulama Okulu, çevrimiçi güvenliğin (e-Güvenlik), bilgisayarlar, tabletler, cep telefonları veya oyun konsolları gibi teknolojiyi kullanırken, dijital dünyadaki çocukların ve yetişkinlerin korunması için vazgeçilmez bir unsur olduğuna inanmaktadır.
- Hüseyin Polat Özel Eğitim Uygulama Okulu, internetin ve bilgi iletişim teknolojilerinin günlük yaşamın önemli bir parçası olduğunu belirtir. Dolayısıyla, riskleri yönetmek ve bunlara tepki vermek için stratejiler geliştirmenin yollarını öğrenmek ve çevrimiçi ortamda esneklik kazanmak için güç sahibi olmak için çocuklar desteklenmelidir.
- Hüseyin Polat Özel Eğitim Uygulama Okulu, eğitim standartlarını yükseltmek, başarıyı teşvik etmek, personelin mesleki çalışmalarını desteklemek ve yönetim işlevlerini geliştirmek için toplumun kaliteli İnternet erişimi sunma yükümlülüğüne sahiptir.
- Hüseyin Polat Özel Eğitim Uygulama Okulu, tüm çocukların ve personelin çevrimiçi olarak potansiyel zararlardan korunmasını sağlamakla sorumludur.
- Hüseyin Polat Özel Eğitim Uygulama Okulu, çevrimiçi güvenlik politikasının amacı şudur:
  - ❖ Hüseyin Polat Özel Eğitim Uygulama Okulu güvenli ve güvenli bir ortam olduğundan emin olmak için, toplumun tüm üyelerinden beklenen ana ilkeleri, güvenli ve sorumlu kullanım teknolojisi ile ilgili olarak tanımlamak.
  - ❖ Hüseyin Polat Özel Eğitim Uygulama Okulu topluluğunun tüm üyelerini çevrimiçi olarak korumak ve güvenliğini sağlamak.
  - ❖ Teknolojinin potansiyel riskleri ve yararları konusunda Hüseyin Polat Özel Eğitim Uygulama Okulu 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.
  - ❖ Okuldaki tüm üyeler tarafından bilinen çevrimiçi güvenlik endişelerine yanıt verirken açıkça kullanılacak prosedürleri tanımlamak.
- Bu politika, 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) dâhil olmak üzere tüm personel için geçerlidir ) yanı sıra çocuklar ve ebeveynler.
- Bu politika, internet erişimi ve kişisel cihazlar da dâhil 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.

#### 1.2Çevrimiçi güvenlik politikası yazma ve gözden geçirme

- Hüseyin Polat Özel Eğitim Uygulama Okulu Online güvenlik politikası, personel, öğrenciler ve ebeveynleri içeren, gerektiğinde uzman tavsiyesi ve katkısı ile okul tarafından yazılmıştır.
- Politika, okul yönetimi tarafından onaylandı ve kabul edildi.
- Okul yönetimi çevrimiçi güvenlik sorumlusu olarak Bilişim Teknolojileri Öğretmeni Hasan Kuzu'yu atadı.
- Okul, online güvenlik (e-Güvenlik) için sorumluluğu üstlenmek üzere okul yönetim kurulu üyesi olarak Müdür Yardımcısını atandı.
- Çevrimiçi güvenlik (e-Güvenlik) Politikası ve uygulaması, en az yılda bir kez veya gerekirse daha erken bir tarihte okul / kurul tarafından gözden geçirilecektir.

## 1.3 Topluluk için kilit sorumluluklar

### 1.3.1 Okul / belirleme yönetimi ve liderlik ekibinin başlıca sorumlulukları şunlardır:

- Çevrimiçi güvenlik vizyonunu ve kültürünü, okul topluluğu boyunca uygun destek ve istişarede bulunarak ulusal ve yerel tavsiyeler doğrultusunda tüm paydaşlara geliştirmek, sahip olmak ve bunları teşvik etmek.
- Çevrimiçi güvenliğin tüm toplum tarafından bir korunma meselesi olarak görülmesini ve güçlü bir çevrimiçi güvenlik kültürünü proaktif olarak geliştirilmesini sağlamak.
- Onların çevrimiçi güvenlik rolü ve sorumluluklarını yerine getirmek için yeterli zaman ve kaynağa sahip olmalarını sağlayarak Belirlenmiş Koruyucu Liderin (DSL) desteklenmesi.
- Çevrimiçi güvenlikle ilgili uygun profesyonel davranışı ve teknolojinin kullanımını kapsayan Kabul Edilebilir Kullanım Politikasını da içeren uygun ve güncel politikaların ve prosedürlerin bulunmasını sağlamak.
- Çocukların gerekli eğitim materyallerine erişmesini sağlamak için okul toplumunun ihtiyaçlarını karşılayan uygun olmayan içerikten çocukları korumak için uygun ve uygun filtreleme ve izleme sistemlerinin kurulmasını sağlamak.
- Okulun / ortam sistemlerinin ve ağlarının güvenliğini ve güvenliğini izlemek ve okul / ortam ağ sisteminin etkin bir şekilde izlenmesini sağlamak için teknik personel ile birlikte çalışmak ve destek sağlamak.
- Tüm personel üyelerinin, çevrimiçi güvenlik rolleri ve sorumlulukları ile ilgili düzenli, güncel ve uygun eğitim almalarının sağlanması ve uygun güvenli iletişimle ilgili rehberlik sağlanması.
- Çevrimiçi güvenliğin tüm öğrencilere çevrimiçi güvenliği, ilgili riskleri ve güvenli davranışları yaşa uygun bir şekilde anlamasını sağlayan ilerici bir bütün okul / öğretim müfredatı içerisinde yer almasını sağlama.
- Çevrimiçi güvenlik olaylarından haberdar olmak ve dış kurumların ve desteğin uygun şekilde irtibatlandırılmasını sağlamak.
- Çevrimiçi korunma kayıtlarını almak ve düzenli olarak gözden geçirmek ve bunları gelecekteki uygulamaları bilgilendirmek ve şekillendirmek için kullanmak.
- Cihazların güvenli ve sorumlu kullanılmasını sağlamak da dâhil olmak üzere, teknolojinin güvenli kullanımı ile ilgili uygun risk değerlendirmelerinin yapılmasını sağlamak.
- Yönetim Organının üyesi olan çevrimiçi güvenliğin sağlanmasına ilişkin sorumluluk üstlenecek bir kişinin sağlanması.

- İyileştirme güç ve alanlarını belirlemek için mevcut çevrimiçi güvenlik uygulamasını denetlemek ve değerlendirmek.
- Belirlenmiş Koruyucu Liderin (DSL), çevrimiçi güvenlik sorumlusu ile birlikte çalışmasını sağlamak.

### **1.3.2 Belirlenmiş Koruyucu Liderin temel sorumlulukları şunlardır:**

- Tüm çevrimiçi korunma konularında adlandırılmış bir irtibat noktası olarak hareket etmek ve diğer personel üyeleri ve diğer ajanslarla uygun şekilde iletişime geçmek.
- Çevrimiçi güvenlikle ilgili mevcut araştırma, mevzuat ve eğilimlerle güncel tutmak.
- Olumlu çevrimiçi davranışı teşvik etmek için yerel ve ulusal etkinliklere katılımı koordine etmek, örneğin Güvenli İnternet Günü.
- Çevrimiçi güvenliğin çeşitli kanallar ve yaklaşımlar vasıtasıyla ebeveynlere ve daha geniş topluluğa tanıtılmasını sağlama.
- Çevrimiçi güvenlik olaylarının ve kayıt yapılarını ve mekanizmalarını koruyan okulların bir parçası olarak alınan önlemlerin kayıtlarını tutmak.
- Okul yönetim ekibine ve diğer birimlere, çevrimiçi güvenlik sorunları ve yerel veriler / rakamlar hakkında rapor vermek.
- Yerel ve ulusal kurumlarla irtibat kurmak.
- Paydaş katkısı ile düzenli olarak çevrimiçi güvenlik politikalarını, Kabul Edilebilir Kullanım Politikalarını (AUP'ler) ve diğer ilgili politikaları gözden geçirmek ve güncellemek için okul / liderlik ve yönetimle birlikte çalışmak.
- Çevrimiçi güvenliğin diğer uygun okul politikaları ve prosedürleriyle bütünleştirilmesini sağlamak.

### **1.3.3 Tüm çalışanların kilit sorumlulukları şunlardır:**

- Çevrimiçi güvenlik politikalarının geliştirilmesine katkıda bulunmak.
- Kabul Edilebilir Kullanım Politikalarını (AUP'lar) okumak ve onlara bağlı kalmak.
- Okul / ortam 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 modelleme
- Mümkün olduğunca müfredat ile çevrimiçi güvenlik eğitimi ilişkilendirme.
- Okul koruma politikalarını ve prosedürlerini takip ederek endişe duyan bireylerin belirlenmesi ve uygun önlem alınması.
- Çevrimiçi güvenlik konusunu ne zaman ve ne kadar içte ve dışta tırmanacağınızı bilmek.
- Çevrimiçi güvenlik konularında, dâhili ve harici olarak, uygun desteğin işaretini koymak.
- Kişisel ve kişisel teknoloji kullanımlarında, hem açık hem de kapalı alanda profesyonel bir davranış seviyesinin korunması.
- Olumlu öğrenme fırsatlarına vurgu yapmak.
- Bu alanda mesleki gelişim için kişisel sorumluluk almak.

### **1.3.4 Yukarıdakilere ilaveten, teknik ortamı yöneten personelin başlıca sorumlulukları şunlardır:**

- Öğrenme fırsatlarının hala en üst düzeye çıkartılmasını sağlarken güvenli online uygulamalarını destekleyen güvenli ve güvenli bir teknik altyapının sağlanması.

- Liderlik ve yönetim ekibi ile ortaklaşa sistemlerin ve verilerin emniyetli bir şekilde uygulanmasının sorumluluğunu üstlenmek.
- Okullara ait cihazlarda tutulan kişisel ve hassas bilgileri korumak için uygun erişim kontrollerinin ve şifrelemenin uygulanmasını sağlamak.
- Okul filtreleme politikasının düzenli olarak uygulanması ve güncellenmesinin sağlanması ve uygulanmasına ilişkin sorumluluğun DSL ile paylaşılması.
- Okulun ağının düzenli olarak izlenmesini sağlamak ve kasıtlı ya da yanlışlıkla yapılan yanlış kullanımı DSL'ye bildirmek.
- Herhangi bir ihlal veya sorunu DSL ve liderlik ekibine rapor etmek ve birlikte kaydedilmesini ve uygun önlemlerin tavsiye edildiği şekilde alınmasını sağlamak.
- Teknik altyapının güvenliği ve güvenliği ile ilgili olarak ilgili mevzuat hakkında bir anlayış geliştirilmesi.
- Herhangi bir ihlali bildirin ve yerel otorite (veya diğer yerel veya ulusal kurumlar) ile teknik altyapı konularında irtibat kurmak.
- Özellikle uygun çevrimiçi güvenlik politikaları ve prosedürlerinin geliştirilmesi ve uygulanmasında DSL ve liderlik ekibine teknik destek sağlamak.
- Okulun BİT altyapısının / sisteminin güvenli olduğunu ve kötüye kullanım veya kötü niyetli saldırılara açık olmamasını sağlamak.
- Tüm ortam makinelerinde ve taşınabilir aygıtlarda uygun anti-virüs yazılımının ve sistem güncellemelerinin kurulmasını sağlamak.
- Uygun olan güçlü parolaların en genç kullanıcıları hariç olmak üzere tümüne uygulandığından emin olmak.

### **1.3.5 Çocukların ve gençlerin başlıca sorumlulukları şunlardır:**

- Çevrimiçi güvenlik politikalarının geliştirilmesine katkıda bulunmak.
- Okulun Kabul Edilebilir Kullanım Politikalarını (AUP'lar) okumak ve onlara bağlı kalmak.
- Çevrim içi ve çevrimdışı başkalarının hislerine ve haklarına saygı duymak.
- İşler ters giderse, güvenilir bir yetiştikenden yardım istemek ve çevrimiçi güvenlik sorunlarıyla karşılaşan diğer kişileri desteklemek.

Bireysel yaşlarına, yeteneklerine ve zayıf yönlerine uygun bir seviyede:

- Kendilerini ve başkalarını çevrimiçi olarak korumak için sorumluluk almak.
- Yeni ve gelişmekte olan teknolojilerin getirdiği fırsatlar ve risklerle ilgili olarak kendi bilinci ve öğrenimlerinden sorumlu olmak.
- Belli bir teknolojiyi kullanmanın kişisel risklerini değerlendirmek ve bu riskleri sınırlamak için güvenli ve sorumluluk sahibi davranmak.

### **1.3.6 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 dięer 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 dięer ağ kaynakları gibi okul sistemlerini güvenli ve uygun bir şekilde kullanmak.
- Yeni ve gelişmekte olan teknolojilerin getirdięi fırsatlar ve risklerle ilgili olarak kendi bilinci ve öğrenimlerinden sorumlu olmak.

## **2. Çevrimiçi İletişim ve Teknolojinin Daha Güvenli Kullanımı**

### **2.1 Okul / web sitesinin yönetilmesi**

#### **Olası beyanlar:**

- 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 sorumluluęunu alacak ve bilgilerin doğru ve uygun olmasını sağlayacaktır.
- Web sitesi, erişilebilirlik fikri mülkiyet haklarına saygı, gizlilik politikaları ve telif hakkı da dâhil 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, uygun bir şekilde güçlü şifreyle şifrelenerek korunacaktır.
- Okul, çevrimiçi güvenlik dâhil olmak üzere, toplumun üyeleri için okul web sitesinde korunma hakkında bilgi gönderecektir.

### **2.2 Çevrimiçi görüntü ve videolar yayınlama**

#### **Olası beyanlar:**

- 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 dięer 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.

### **2.3 Eğitim amaçlı resmi video konferans ve web kamerası kullanımı**

#### **2.3 Olası beyanlar:**

- 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 cevaplama ayarlanmayacaktır.
- Harici IP adresleri dięer 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.

## **2.4 İnternetin ve ilgili cihazların uygun ve güvenli derslik kullanımı**

### **2.4 Olası beyanlar:**

- 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 / ortamın 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.
- Öğrencilerin yaşlarına ve yeteneklerine uygun olacaktır.
- Genç öğrencilerin İnternet'e erişimi, yetişkinlerin gösteri yaparak, öğrencilerin yaşı ve yeteneği için planlanan öğrenme çıktılarını destekleyen belirli ve onaylanmış çevrimiçi materyallere doğrudan denetlenen erişimle sağlanacaktır.
- 8-11 yaşındaki öğrenci denetlenecek. Öğrenciler yaşa uygun arama motorlarını ve çevrimiçi araçları kullanacak ve çevrimiçi etkinlikler gerektiğinde öğretmen tarafından yönlendirilecek. Çocuklar, öğrencilerin yaşı ve yeteneği için planlanan öğrenme çıktılarını destekleyen çevrimiçi materyal ve kaynaklara yönlendirilecektir.
- Yetenek ve anlayışlarına göre, genç öğrenciler teknoloji kullanırken uygun bir şekilde gözetim altına alınacaklardır.
- 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 dâhil 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 düşünceleri 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.

## **3. Kişisel Cihazların ve Cep Telefonlarının Kullanımı**

### **3.1 Kişisel cihazlar ve cep telefonları ile ilgili gerekçe**

### **3.1 Olası Bildirimler:**

- Cep telefonlarının ve çocukların, gençlerin ve yetişkinler arasındaki diğer kişisel cihazların yaygın bir şekilde sahiplenilmesi, tüm üyelerin Hüseyin Polat Özel Eğitim Uygulama Okulu 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 dâhil olmak üzere uygun politikalarda yer alacaktır.
- Hüseyin Polat Özel Eğitim Uygulama Okulu, 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.

### **3.2 Kişisel cihazların ve cep telefonlarının güvenli bir şekilde kullanılması için beklentiler**

#### **3.2 Olası Bildirimler:**

- 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.
- Hüseyin Polat Özel Eğitim Uygulama Okulu topluluğunun tüm üyelerine cep telefonlarını veya cihazlarını kayıp, hırsızlık veya hasardan korumak için adım atmaları önerilir.
- Hüseyin Polat Özel Eğitim Uygulama Okulu topluluğunun 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.
- Hüseyin Polat Özel Eğitim Uygulama Okulu 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.

### **3.3 Öğrencilerin kişisel cihazlarını ve cep telefonlarını kullanımı**

#### **3.3 Olası Bildirimler:**

- Öğrenciler, kişisel cihazların ve cep telefonlarının güvenli ve uygun kullanımı konusunda eğitim alacaklardır.
- Çocukların cep telefonlarının ve kişisel cihazların tüm kullanımları, kabul edilebilir kullanım politikasına uygun olarak gerçekleşecektir.
- 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 kullanılamaz.
- Çocukların cep telefonlarını veya kişisel cihazlarını eğitim etkinliğinde kullanımı, okul idaresi tarafından onaylandığında gerçekleşecektir.

- Bir öğrenci ebeveynlerini arama gereği duyduğunda, okul telefonunu kullanmasına izin verilecektir.
- Ebeveynlerin okul saatlerinde cep telefonu ile çocuklarıyla iletişim kurmamaları, okul idaresine başvuruları 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.

### **3.4 Kişisel cihazların ve cep telefonlarının personel kullanımı**

#### **3.4 Olası Bildirimler:**

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

### **3.5 Ziyaretçiler kişisel cihazların ve cep telefonlarının kullanılması**

#### **3.5 Olası Bildirimler:**

- 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.



## 4. Politika Kararları

### 4.1. Çevrimiçi riskleri azaltmak

#### 4.1 Olası beyanlar:

- Hüseyin Polat Özel Eğitim Uygulama Okulu internetin yeni uygulamalar, araçlar, cihazlar, siteler ve materyallerin hızla geliştiği sürekli değişen bir ortam olduğunun farkındadır.
- Gelişen teknolojiler eğitimsel fayda açısından incelenecek ve okul liderliği ekibi, okulda kullanılmasına izin verilmeden önce uygun risk değerlendirmelerinin yapılmasını sağlayacaktır.
- Okul, personelin ve öğrencilerin uygun olmayan veya yasadışı içeriğe erişmesini önlemek için uygun filtreleme ve izleme sistemlerinin kurulmasını sağlayacaktır.
- Okul, kullanıcıların yalnızca uygun materyallere erişmesini sağlamak için makul önlemleri alacaktır. Bununla birlikte, internet içeriğinin küresel ve bağlanmış niteliğinden dolayı, uygun olmayan materyallerin bir okul / bilgisayar ya da cihaz vasıtasıyla hiçbir zaman gerçekleşmeyeceğini garanti etmek her zaman mümkün değildir.
- Okul, çevrimiçi güvenlik (e-Güvenlik) politikasının yeterli olup olmadığını ve politikanın uygulanmasının uygun olup olmadığını belirlemek için teknolojinin kullanımını denetleyecektir.
- Çevrimiçi riskleri belirleme, değerlendirme ve azaltma yöntemleri okul liderliği ekibi tarafından düzenli olarak incelenecektir.

### 4.2. Daha geniş çapta okul / toplum ortamında internet kullanımı

#### 4.2 Olası beyanlar:

- Okul, çevrimiçi güvenlik konusunda ortak bir yaklaşım oluşturmak için yerel kuruluşlarla irtibat kuracak.
- Okul, internet kullanımının uygun olmasını sağlamak için yerel topluluğun ihtiyaçları (kültürel geçmişleri, dilleri, dinleri ve etnik kökenleri tanımayı da içeren) ile çalışacaktır.
- Okul, okul bilgisayar sistemine veya sitedeki internete erişmesi gereken herhangi bir konuk / ziyaretçi için Kabul Edilebilir Kullanım Politikası sağlayacaktır.

### 4.3 İnternet erişiminin yetkilendirilmesi

#### 4.3 Olası beyanlar:

- Okul, okulun cihaz ve sistemlerine erişim izni verilen tüm personelin ve öğrencilerin güncel bir kaydını tutacaktır.
- Tüm personel, öğrenciler ve ziyaretçiler, herhangi bir okul kaynaklarını kullanmadan önce Kabul Edilebilir Kullanım Politikasını okuyacak ve imzalayacaklardır.
- Ebeveynlere, öğrencilere, yaşlarına ve yeteneklerine uygun denetlenen İnternet erişimi sağlanacakları bildirilecektir.
- Ebeveynlerden, öğrencilerin erişebilmesi için Kabul Edilebilir Kullanım Politikasını okumaları ve uygun olduğunda, çocuklarıyla tartışmaları istenecektir.
- Toplumun savunmasız üyeleri için (özel eğitim gereksinimi olan çocuklar gibi) erişimi düşünürken, okul öğrencilerin belirli ihtiyaçları ve anlayışları temelinde kararlar alacaktır.

## 5. Katılım Yaklaşımları

### 5.1 Çocukların ve gençlerin katılımı ve eğitimi

#### 5.1 Olası beyanlar:

- 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 dâhil 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.
- Çevrimiçi güvenlik (e-Güvenlik) PSHE, SRE, Citizenship and Computing / BİT programlarına dâhil edilecek ve hem güvenli okul hem de evde kullanımını kapsayacaktır.
- Kabul Edilebilir Kullanım beklentileri ve Posterler, İnternet erişimi olan tüm odalarda yayınlanacaktır.
- İnternetin ve teknolojinin güvenli ve sorumlu kullanımı, müfredatta ve tüm konularda güçlenecektir.
- Dışarıdan destek, okulların dâhili 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 eğitimi uygulayacaktır.

## **5.2 Savunmasız kabul edilen çocukların ve gençlerin katılımı ve eğitimi**

### **5.2 Olası ifade:**

Hüseyin Polat Özel Eğitim Uygulama Okulu, bir takım faktörlerden dolayı bazı çocukların çevrimiçi ortamda daha savunmasız olduğunu düşünmektedir.

## **5.3 Personelin katılımı ve eğitimi**

### **5.3 Olası beyanlar:**

- 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.

## 5.4 Ebeveynlerin katılımı ve eğitimi

### 5.4 Olası beyanlar:

- Hüseyin Polat Özel Eğitim Uygulama Okulu, 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.
- Çevrimiçi güvenlik konusundaki ebeveynler için bilgi ve rehberlik, ebeveynlere çeşitli biçimlerde sunulacaktır.
- Ebeveynlerin, çevrimiçi olarak çocukları için olumlu davranışları rol modellemeleri teşvik edilecektir.

## 6. Çevrimiçi Olaylara ve Koruma sorunlarına yanıt verme

### Olası beyanlar:

- Okulun tüm üyeleri, cinsel içerikli mesajlaşma, çevrimiçi / siber zorbalık vb. dâhil olmak üzere karşılaşılabilecek çevrimiçi risklerin çeşitliliğinden haberdar edilecektir. Bu, öğrencilere yönelik personel eğitimi ve eğitim yaklaşımları içerisinde vurgulanacaktır.
- Okulun 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, okulun şikâyet prosedürleri kapsamında ele alınacaktır.
- Çevrimiçi / siber zorbalık ile ilgili şikâyetler, okulun zorbalık karşıtı politikası ve prosedürü kapsamında ele alınacak
- Personelin yanlış kullanımı ile ilgili herhangi bir şikâyet okul müdürüne yönlendirilecektir.
- Okul şikâyet prosedürü öğrencilere, velilere ve personele bildirilecektir.
- Şikâyet 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 diğfer 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.