**DR.HAYDAR ASLAN İLKOKULU**

**2022-2023 EĞİTİM ÖĞRETİM YILI E-SAFETY (E-GÜVENLİK) POLİTİKASI**

**E-GÜVENLİK VİZYONUMUZ**

Okulumuzun e-güvenlik vizyonu, dijital ortamların hızla geliştiği ve yayıldığı bir zaman diliminde dünyaya gelen ve bu dünya ile iç içe büyüyen öğrencilerimizin bu ortamlarda güvenli kalmalarını sağlamak ve ek olarak bilinçli ve bilgili birer medya okur yazarı olarak yetişmelerini amaçlamaktır.

**Okulumuz e-Safety (e-güvenlik ) Politikası ve Amaçları**

Teknolojinin hızla geliştiği günümüze her okulun Okul Güvenlik Politikası’nın olması zorunlu hale gelmiştir. Günlük hayatımızın bir parçası olarak hepimiz dijital teknolojilerle yaşıyoruz. Hedef grubumuz olan öğrencilerimiz başta olmak üzere okulumuz paydaşlarına teknolojiden en yüksek yararı sağlarken bilinçli ve güvenli teknoloji kullanımını öğretmek zorundayız. Bütün okul bileşenleri olarak internet kullanımının en güvenli şekilde ve en güvenli ortamda yapılmasını sağlamayı amaçlıyoruz. Bu nedenle personel, öğrenci ve velileri için açık ve anlaşılır Güvenli İnternet Okul Politikası’na sahibiz.

**A. E-SAFETY (E-GÜVENLİK) POLİTİKAMIZ**

* Okulumuzun internet sitesi, twitter gibi sosyal ağlarda hesapları bulunmaktadır. Bu ağlar üzerinde yayınlanan veriler kontrollü olarak paylaşılmaktadır.
* Rehberlik servisi tarafından ve BİT Öğretmeni tarafından sınıflara düzenli olarak, teknoloji bağımlılığı, BİT’nin doğru ve güvenli kullanımı, siber zorbalık gibi konularda seminerler düzenlenmektedir.
* Okulumuzda BİT doğru ve güvenli kullanımı ile ilgili sabit panolar bulunmaktadır.
* Okulumuzun bazı öğretmenleri Milli Eğitim Bakanlığı tarafından ve etwinningonlineeba üzerinden verilen BİT’in doğru ve güvenli kullanımı, e-Safety Label konularında uzaktan ve yüz yüze eğitimler almıştır.
* Okulumuzda her yıl “ Güvenli İnternet Günü (E-Safety Day)” kutlanmaktadır. Okulumuzda güvenli internet günü kutlamalarında, konu ile ilgili seminerlerde güvenliweb.org.tr. sitesinden alıntılanan bilgi broşürleri dağıtılmaktadır.
* Okulumuzun internet sitesinde e-güvenlik konusunda bir bölüm bulunmaktadır. Burada çeşitli bilgilendirmeler ve bağlantılar mevcuttur. Okul paydaşlarımız istedikleri zaman konu ile ilgili bilgi alabilmekteler.
* Rehber Öğretmenlerimiz internet etiği ve güvenli internet kullanımı konuları hakkında öğrencilerimize bilgilerini aktarmaktadır. Bu konu her yıl sınıfların Rehberlik Çerçeve Planı’nda yer almaktadır.
* Okulumuzda 21.yy iletişim becerileri önemsenmektedir. Bununla ilgili olarak öğrencilerimizin BİT kullanım becerilerini geliştirme çalışılmaları yapılmaktadır.
* Uygun profesyonel davranış ve teknoloji kullanımını kapsayan Kabul Edilebilir Kullanım Politikası (AUP) dahil olmak üzere çevrimiçi güvenliğe ilişkin uygun ve güncel politika ve prosedürleri sağlamak.
* Okulumuzda yürütülen eTwinning ve diğer projelerde bu konuda etkinliklere yer verilmektedir.
* Okulumuzda Dijital vatandaş olma konusunda paydaşlarımızı bilinçlendirme çalışmaları yapılmaktadır.

**B. OKULUMUZDA E-GÜVENLİK POLİTİKASININ AMACI**

* Okulumuzun tüm üyelerini çevrimiçi olarak korumak ve güvenliğini sağlamak.
* Teknolojinin potansiyel riskleri ve yararları konusunda idareci,öğretmen, 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 yönetici, öğretmenler, destek personeli, kantinciler, okul aile birliği, ziyaretçiler, gönüllüler ve okul adına hizmet veren veya bunları yerine getiren diğer kişiler, çocuklar ve ebeveynleri kapsamasını sağlamaktır.

**C. OKULUMUZ ÇALIŞANLARININ BAŞLICA SORUMLULUKLARI**

* Çevrim içi güvenlik politikalarının geliştirilmesine katkıda bulunmak.
* Okul sistemlerinin ve verilerin güvenliğinden sorumlu olmak.
* Yeni ve gelişmekte olan teknolojilerin kullanıldığı iyi uygulamaları öğrenmek.
* Mümkün olduğunca müfredat ile çevrimiçi güvenlik eğitimini ilişkilendirmek.
* Okul koruma politikalarını ve prosedürlerini takip ederek endişe duyan bireyleri belirlemek ve önlem almak.
* Olumlu öğrenme fırsatlarına vurgu yapmak. Bu alanda mesleki gelişim için kişisel sorumluluk

almak.

**ÖĞRENCİLERİMİZİN BAŞLICA SORUMLULUKLARI**

* Çevrim içi güvenlik politikalarının geliştirilmesine katkıda bulunmak.
* Çevrim içi ve çevrim dışı başkalarının hislerine ve haklarına saygı duymak.
* İşler ters giderse, güvenilir bir yetişkinden yardım istemek ve çevrimiçi güvenlik sorunlarıyla karşılaşan diğer kişileri desteklemek.
* Kendilerini ve başkalarını çevrimiçi olarak korumak için sorumluluk almak.
* Yeni ve gelişmekte olan teknolojilerin getirdiği fırsatları ve riskleri bilmek.
* Teknolojiyi kullanmanın kişisel risklerini bilmek.
* Uzaktan eğitim durumlarında yapması ve yapmaması gerekenlerin farkında olmak

**VELİLERİMİZİN BAŞLICA SORUMLULUKLARI**

* 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 veya 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.
* Uzaktan eğitim durumlarında çocuklar için verimli geçirilmesi için çevrimiçi etkinliklere katılımını sağlamak.
* Uzaktan eğitim durumlarında çocukları için olumlu etkinliklere yöneltmek ve tüm personelle bu konuda iletişime geçmeye hazır olmak.

**D. 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 web siyesi yönetme yayın komisyonumuz vardır.
* Web sitesi, erişilebilirlik fikri mülkiyet haklarına saygı, kvkk 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 öğrencilerinizle ya da ebeveynlerinizle yayınlanacaktır.
* Okul web sitesinin yönetici hesabı, uygun bir şekilde güçlü şifreyle şifrelenerek korunacaktır.
* Okul, çevrim içi güvenlik dahil olmak üzere, toplumun üyeleri için okul web sitesinde korunma hakkında bilgi gönderecektir.

**Çevrimiçi Görüntü Ve Videolar Yayınlama :**

* Okulda, çevrimiçi paylaşılan tüm resimlerin ve videoların okulun çevrimiçi güvenlik ( e-Güvenlik) politikasına uygun şekilde kullanılması sağlanacaktır.
* Okulda, resimlerin ve videoların kullanımı, veri güvenliği,davranış kuralları, sosyal medya, kişisel cihazların ve cep telefonlarının kullanımı gibi diğer politikalar ve prosedürlere uygun şekilde yapılacaktır.
* Çevrimiçi güvenlik(e-Güvenlik)politikasına uygun olarak, öğrencilerin resimlerinin/videolarının elektronik olarak yayınlanmasından önce her zaman ebeveynlerin yazılı izni alınacaktır. (Sosyal Medya İzin Belgesi)
* Öğrenciler, bir video konferans araması veya mesajı hazırlamadan veya cevaplamadan önce bir öğretmenin izin isteyecektir.
* Video konferans, öğrencilerin yaşı ve yeteneği için uygun bir şekilde denetlenecek.
* Velilerin rızası, çocuklar video konferans faaliyetlerine katılmadan önce alınacaktır.
* Video konferans, sağlam bir risk değerlendirmesini takiben, resmi ve onaylanmış iletişim kanalları vasıtasıyla gerçekleşecektir.
* Sadece ana yöneticilere video konferans yönetim alanlarına veya uzaktan kumanda sayfalarına erişim hakkı verilecektir.
* Eğitimsel video konferans servisleri için özel oturum açma ve şifre bilgileri yalnızca personellere verilecek ve gizli tutulacaktır.
* Öğretmen ve öğrencilerimiz okulda sadece Milli Eğitim Bakanlığının denetimindeki internet ağını kullanabilirler.
* Okulumuz internet ağına MEB SERTİFİKA güvenlik dosyası yüklenmeden internet ağına bağlanılamaz.
* Okul içerisinde proje için bile olsa sadece öğretmenlerin kayıtlı cihazları kullanılır.
* E-güvenlik politikamız Milli Eğitim Bakanlığı tarafından yayınlanan güvenli internet çerçevesine dâhildir. ( Milli Eğitim Bakanlığı 2017/12 Sayılı Genelge)
* Çalışanların tüm üyeleri, çocukları korumak için tek başına filtrelemeye güvenmeyeceklerinin farkındadır ve gözetim, sınıf yönetimi ve güvenli ve sorumlu kullanım eğitimi önemlidir.
* Tüm okul ait cihazlar, okulun Kabul Edilebilir Kullanım Politikasına uygun olarak ve uygun güvenlik ve güvenlik önlemleri alınarak kullanılacaktır.

**İnternetin Ve İlgili Cihazların Uygun Ve Güvenli Kullanımı :**

* İnternet kullanımı eğitimsel erişimin önemli bir özelliğidir ve tüm çocuklar bütünleşik okul müfredatının bir parçası olarak sorunlarını yanıtlamak için stratejiler geliştirmelerini destekleyecek ve onlara yardımcı olacak yaşa ve yeteneğe uygun eğitim alacaklardır.
* Okulun 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 , güvenli ve sorumlu kullanım eğitimi önemlidir.
* Tüm okula ait cihazlar, uygun güvenlik ve güvenlik önlemleri alınarak kullanılacaktır.
* Personel, 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 internetten türetilen materyallerin telif hakkı yasalarına uygun olmasını ve bilgi kaynaklarını kabul etmesini sağlayacaktır.
* Öğrencilere, okudukları veya gösterilen bilgilerin doğruluğunu kabul etmeden önce eleştirel düşünmeleri öğretilecektir.
* Çevrimiçi materyallerin değerlendirilmesi, her konuda öğretme ve öğrenmenin bir parçasıdır ve müfredatta bir bütün olarak görülür.
* Okul, öğrencileri ve çalışanlarımızın güvenli ve gizli bir ortamda iletişim kurmalarını ve iş birliği yapmalarını sağlamak için interneti kullanacaklardır.

**Kişisel Cihazların ve Cep Telefonlarının Kullanımı :**

* Okulumuzda yetişkinlerin cep telefonlarının ve diğer kişisel cihazların kullanımı, okul tarafından belirlenen Cep Telefonu Kullanım Politikası kurallarına göre sağlanacaktır.
* Okulumuz, 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 kullanılması için gerekli önlemleri almak zorundadır.
* Kişisel cihazların ve cep telefonlarının kullanımı yasaya ve diğer uygun okul politikalarına uygun olarak yerine getirilecektir.
* Okula getirilen her türlü elektronik cihazın sorumluluğu kullanıcıya aittir.
* Okul, bu tür cihazların kaybı, çalınması veya zarar görmesi konusunda sorumluluk kabul etmez.
* Kötüye kullanım, uygun olmayan mesajların veya içeriğin bu cihazlarla gönderilmesi durumunda disiplin politikası kuralları uygulanacaktır.
* Okulun tüm üyelerine, kayboldukları veya çalındığı takdirde telefonlarında veya cihazlarında yetkisiz aramaların yapılmaması için şifre kullanmaları önerilir.
* Okulun tüm üyelerine, cep telefonlarının ve kişisel cihazlarının saldırgan, küçümseyen veya başka şekilde okul politikalarına aykırı düşen herhangi bir içerik içermediğinden emin olmaları önerilir.

**Öğrencilerin Kişisel Cihazlar ve Cep Telefonları Kullanımı :**.

* Cep telefonları veya kişisel cihazlar, öğrencilerin bir öğretmen onayını alarak onaylanmış ve müfredat tabanlı etkinlik kapsamında olmadıkları sürece dersler veya resmi okul saatlerinde öğrenciler tarafından kullanılamaz.
* Öğrencilerimiz yaş itibari ile ilkokul seviyesinde oldukları için okula cep telefonu, tablet ve bilgisayar getirmeyeceklerdir ama kullanım konusunda eğitim alacaklardır
* 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 telefonuyla çocuklarıyla iletişim kurmamaları, okul idaresinin izni ile gerçekleştirilmelidir.

**Personelin Kişisel Cihazlar Ve Cep Telefonları Kullanımı :**

* Personelin kişisel cep telefonları ve cihazları ders saatlerinde kapatılır veya sessiz moda geçirilir.
* Bluetooth veya diğer iletişim biçimleri ders saatlerinde "gizlenmiş" veya kapalı olmalıdır.
* 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, güvenlik güçlerine bildirilecektir.
* Personelin cep telefonunu veya cihazlarını kişisel olarak kullanmalarını içeren herhangi bir iddiaya okul yönetim politikasını izleyerek yanıt verilecektir.

**Çocukların 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.
* Tüm kullanıcılara ağ ve internet kullanımının izleneceği bildirilecektir.
* Posterler, e güvenlik panoları okulun çeşitli yerlerinde sergilenecektir.
* 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 tek bir kullanıcıya kadar izlenebileceğinin farkında olacak.
* Personelin tüm üyelerine, profesyonel ve kişisel olarak, güvenli ve sorumlu İnternet kullanımı konusunda güncel ve uygun personel eğitimi, düzenli (en az yıllık) olarak sağlanacaktır.
* Personel, çevrimiçi davranışlarının okulun itibarını etkileyebileceğinin farkına varacaktır.
* Filtreleme sistemlerini yönetme veya BİT kullanımını izleme sorumluluğu taşıyan personel, okul yönetimi tarafından denetlenecektir.
* Okul, çalışanların öğrencilerin yaşlarına ve yeteneklerine göre kullanması gereken yararlı çevrimiçi araçları sağlayacaktır.

**Ebeveynlerin Katılımı ve Eğitimi**

* Dr.Haydar Aslan İlkokulu, çocukların internetin ve dijital teknolojinin güvenilir ve sorumlu kullanıcıları olabilmesi için ana-babaların önemli bir role sahip olduklarını kabul eder.
* Ebeveynlerin dikkatleri, okul açıklamaları ve okul web sitesinde okul çevrimiçi güvenlik (e-Güvenlik) politikasına ve beklentilerine yönelecektir.
* 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, cinsel içerikli mesajlaşma, çevrimiçi / siber zorbalık vb. dahil olmak üzere karşılaşılabilecek çevrimiçi risklerin çeşitliliğinden haberdar edilecektir.
* Okulun tüm üyeleri, filtreleme, cinsel içerikli mesajlaşma, siber zorbalık, yasadışı içerik ihlali vb. gibi çevrimiçi güvenlik (e-Güvenlik) endişelerini bildirme prosedürü 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 alınacaktır.
* Personelin yanlış kullanımı ile ilgili herhangi bir şikâyet okul yönetimine 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 paydaşlarının herhangi bir diğer üyesine zarar vermek, sıkıntı yaşamak veya suç oluşturan herhangi bir içerik, yorum, resim veya video yayımlamamanın önemini hatırlatacaktır.
* Okul, çevrimiçi güvenlik (e-Güvenlik) olaylarını, uygun olduğunda, okul disiplini /davranış politikasına uygun olarak yönetir.
* Okul, ebeveynlere, ihtiyaç duyulduğunda bunlarla ilgili endişeleri bildirir.
* Herhangi bir soruşturma tamamlandıktan sonra okul bilgi alacak, öğrenilen dersleri belirleyecek ve değişiklikleri gerektiği gibi uygulayacaktır.
* Paylaşılan içeriklerden emin olmak için teyit.org Türkiye merkezli Türkçe bir doğrulama platformu kullanılması önerilir.
* Sorunları çözmek için ebeveynlerin ve çocukların okulla ortak çalışması gerekir.

**E. Kabul Edilebilir Kullanım Politikası**

Dr.Haydar Aslan İlkokulu bilgisayar sistemlerini yüzlerce kullanıcı paylaşmaktadır. Bu sistemler dikkatli bir şekilde kullanılmalıdır; bir kaç kişinin hatalı kullanımı bile okulun ve diğer kişilerin çalışmalarını sekteye uğratma potansiyeline sahiptir. Bu sebeple kullanıcılar okulun bilgisayar sistemlerini kullanırken dikkatli olmalı ve etik davranış sergilemelidir. Bu yükümlülük, aşağıdakilerle sınırlı olmamakla birlikte şunları kapsamaktadır:

* Dr.Haydar Aslan İlkokulu ,okula ait bilgisayar sistemleri üzerindeki tüm hak, mülkiyet ve çıkarlara sahiptir. Kabul Edilebilir Kullanım Politikası veya bilgisayar sistemlerin kullanımına ilişkin olarak okul tarafından herhangi bir mecrada yayımlanan hüküm ve koşullar altındaki hiçbir hüküm hiçbir şekilde söz konusu hak, mülkiyet ve çıkarların kullanıcılara devredildiği anlamına gelmemektedir. Okul 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 üretemez, bunlardan türemiş çalışma yaratamaz, tersine mühendislik yapamaz, parçalara ayıramaz veya diğer bir şekilde kaynak koduna dönüştüremez.
* Kullanıcılar, okulun 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 Okul’un bilgisayar sistemlerini kullanamaz.
* Kullanıcılar, Okul hesaplarını kullanması için hiç kimseyi hiçbir sebeple yetkilendiremez. Okul 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 işlemden, söz konusu işlemi gerçekleştiren taraf hesap sahibinin kendisi olmasa dahi sorumlu hesap sahibidir.
* Okulun bilgisayar sistemleri yalnızca izin verildiği şekilde Okul ile ilişkili hususlarda kullanılmalıdır. Tüm Okul donanımı için söz konusu olduğu üzere, okul ağı dâhil bilgisayar sistemlerinin şahsi veya ticari amaçlar doğrultusunda kullanılması, açıkça izin verilmeyen haller dışında yasaktır. Okulun 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 Üniversite hem de söz konusu ağ ve hizmetleri sunan kuruluşlar tarafından yayımlanan kabul edilebilir kullanım politikalarına uygun olmalıdır.
* Kullanıcılar Okulun ilgili personeli, bilgi güvenliği sorumlusu veya ilgili taraftan önceden izin almadıkça, herhangi bir bilgiye, Okula 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.
* Okula ait hiçbir bilgisayar sistemi sorumsuz bir şekilde veya başkalarının işlerine engel olacak şekilde kullanılamaz. Buna; hakaret içerikli, rahatsız edici veya taciz edici içerikler ile zincirleme mektup, yetkisiz toplu mail veya istenmeyen reklamların iletilmesi veya ulaşılabilir 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.
* Okul, 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. Okul, üçüncü taraf içeriklerinin doğru, tam ve güvenilir olduğuna ilişkin her türlü yükümlülükten kendini muaf tutmaktadır. Kullanıcı bilgisayar sistemlerinde bulundurduğu veya sakladığı bilgilerden kendisi sorumludur.

 E GÜVENLİK KOMİSYONU

ELİF ÖNDER TUBA KARAYİĞİT MUSTAFA BİRİNCİ

MÜDÜR YARD. İNGİLİZCE ÖĞRT. BİT ÖĞRETMENİ

SAFİYE AKKAYA GAMZE ÇAĞLAR

SINIF ÖĞRETMENİ REHBER ÖĞRETMEN

20/09/2022

Bülent GELİBOLU

Okul Müdürü