

DARICA DEDE KORKUT İLKOKULU

e-GÜVENLİK OKUL EYLEM PLANI

Bilgi ve iletişim teknolojileri (BİT), kalkınmanın hızlandırıcısı ve lokomotifleri olarak yaşadığımız dijital çağda büyük bir öneme sahiptir. Gelişen bilgi ve iletişim teknolojileri, üretim, sağlık ve eğitim gibi hayatın her alanına dokunmakta ve toplumların refah seviyelerinin yükselmesini sağlamaktadır. Tüm vatandaşlarımızın internetin getirmiş olduğu fırsatlardan sonuna kadar yararlanabilmelerinin sağlanmasının yanı sıra başta çocuklarımızın internetin zararlı içeriklerinden korunmaları gerekmektedir.

Okulumuz çocukların internet teknolojilerini belirli bir sorumluluk ve bilinç dâhilinde kullanmalarını sağlamak için bilinçlendirme faaliyetlerinde bulunmakta, bu kapsamda internetin yasadışı ve zararlı içerikleri ile mücadele konusunda eğitim-öğretim faaliyetlerini sürdürmekte; riskleri yönetmeleri ve bunlara tepki vermek için stratejiler geliştirmenin yollarını öğrenmeleri için çocukları desteklemektedir.

Darıca Dede Korkut İlkokulu olarak, 21. Yüzyıl becerilerinin kazanılması ve çağın gerekliliklerine hazır öğrenciler yetiştirmek için her türlü teknolojiyi kullanırken, aynı zamanda öğrencilerimize güvenli bir ortam hazırlamanın gerekliliğine inanıyoruz. İnternet kullanımını artarken, öğrencilerimize güvenli bir ortam sağlamak gerektiğinin, güvenli ortamları bulmak için çözümler aramamız gerektiğinin farkındayız.

Bu bilinçle çevrimiçi ortamda karşılaşılan riskler konusunda öğrenci, öğretmen veli ve çalışanlarımızı bilinçlendirmek üzere çeşitli çalışmalar yapmaktayız. Öğrencilerimizin evde, okulda veya dışarıda ya da arkadaşlarıyla ya da yalnız olduğu zaman, onu koruyacak önlemleri alan, Güvenli İnternet Okul Politikasına sahip bir okuluz.

Okulumuz, okul çapında bir zorbalık önleme programının oluşturulmasını kolaylaştıracak politikalar oluşturur. Başarılı ve etkili programlar, bireysel öğrencilerden ve sınıflardan, eğitimcileri ve öğrencileri birleştiren zorbalık karşıtı takımlara kadar, okulda her seviyede zorbalık karşıtı stratejileri teşvik etmek için çalışır.

Ayrıca okulumuz velilerimizi, öğrencilerimizi dijital mahremiyetin korunması, veri gizliliği, dijital ayak izi vb. konularda bilinçlendirme çalışmaları yaparak, güvenli internet ortamı sağlamayı amaçlar.

AMAÇ VE KAPSAM:

Bu politikanın amacı, Darıca Dede Korkut İlkokulu Bilgisayar Sistemleri'nin kullanım koşullarını ve kabul edilebilir kullanım politikasını belirlemektir.

Dede Korkut İlkokulu , 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.

Dede Korkut İlkokulu , internetin ve bilgi iletişim teknolojilerinin günlük yaşamın önemli bir parçası olduğuna inanır. Dolayısıyla, riskleri yönetmeleri ve bunlara tepki vermek için stratejiler geliştirmenin yollarını öğrenmeleri için çocuklar desteklenmelidir.

Dede Korkut İlkokulu, eğitim standartlarını yükseltmek, başarıyı teşvik etmek, personelin mesleki çalışmalarını desteklemek ve yönetim işlevlerini geliştirmek için toplumun kaliteli İnternet erişimi sunma yükümlülüğüne sahiptir.

Dede Korkut İlkokulu, tüm çocukların ve personelin çevrimiçi olarak potansiyel zararlardan korunmasını sağlamakla sorumludur.

- Okulumuzun tüm üyelerini çevrimiçi olarak korumak ve güvenliğini sağlamak.
- Teknolojinin potansiyel riskleri ve yararları konusunda Dede Korkut İlkokulu idarecileri, öğretmenleri, öğrencileri ve çalışanları için farkındalık yaratmak.
- Tüm personelin güvenli ve sorumlu bir şekilde çalışmasını sağlamak, olumlu davranışları online olarak modellemek ve teknolojiyi kullanırken kendi standartlarını ve uygulamalarını yönetme gereksiniminin farkında olmak.
- Okuldaki tüm üyeler tarafından bilinen çevrimiçi güvenlik endişelerine yanıt verirken açıkça kullanılacak prosedürleri tanımlamak.
- Bu politikanın, yönetim organı, öğretmenler, öğrenciler, veliler, destek personeli, harici yükleniciler, ziyaretçiler, gönüllüler ve okul adına hizmet veren veya bunları yerine getiren diğer kişiler (toplu olarak bu politikada 'personel' olarak anılacaktır) dahil olmak üzere tüm personel için 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. Çocuklar, personel ya da diğer kişilere, çalıştıkları dizüstü bilgisayarlar, tabletler veya mobil cihazlar gibi uzaktan kullanım için okul tarafından verilen cihazlar için de geçerlidir.

e- GÜVENLİK HAKKINDA ALINAN KARARLAR

1 . Mihver ve serbest etkinlik derslerinde ve rehberlik derslerinde güvenli internet kullanımı ile ilgili kazanımlar eklenmesine,

- Türkçe, Hayat Bilgisi, Fen Bilimleri, Sosyal Bilimler vb. ilgili derslerde uygun şekilde işlenmesi sağlanmalıdır.

2. Çocuklarda bilinçli ve güvenli internet kullanımına dair bilgi, beceri ve tutumların geliştirilmesi için seminerler düzenlenmesine, karar verilmiştir.

- Okulumuzda güvenli internet ağı mevcuttur.
- Okulumuzda elektromanyetik kirliliğe ve internet güvenliğine önem verilmektedir.

3. Okulumuzda ders anlatımı yapılan her alanda etkileşimli tahta ve güvenli internet erişim ağı vardır. Ders anlatımlarında eba eğitim ve eTwinning portallarından da yararlanılmaktadır. Güvenli internet erişim ağı, ağ güvenlik filtresiyle kullanılmaktadır.

4. Okulumuzun internet sitesi, Instagram, facebook gibi sosyal ağları bulunmaktadır. Bu ağların üzerinde yayınlanan veriler kontrollü olarak paylaşılmaktadır.
5. Etkileşimli tahtalar güvenlik kurulumu ile öğretmenlerin kontrolünde kullanılmaktadır.
6. Okulumuzda 21.yy iletişim becerileri önemslenmektedir. Bununla ilgili olarak öğrencilerimizin BİT kullanım becerilerini geliştirme çalışmaları yapılmaktadır.
7. Okulumuzda Dijital vatandaş olma konusunda paydaşlarımızı bilinçlendirme çalışmaları yapılmaktadır.
8. Okulumuzda BİT doğru ve güvenli kullanımı ile ilgili sabit panolar bulunmaktadır.
9. Rehberlik servisi tarafından, sınıflara düzenli olarak, BİT bağımlılığı, BİT'nin doğru ve güvenli kullanımı, Siber Zorbalık gibi konularda seminerler düzenlenmektedir.
10. Okulumuzun bazı öğretmenleri Milli Eğitim Bakanlığı tarafından verilen Siber Zorbalık, BİT 'in doğru ve güvenli kullanımı konularında uzaktan ve yüz yüze eğitimler almıştır.
11. Okulumuzda Şubat ayında " Güvenli İnternet Günü" kutlanmaktadır.
12. Okulumuzda izinsiz fotoğraf çekmek kesinlikle yasaktır.
13. Okulumuzun öğrencilerinin yüzleri eTwinning portalı dahilindeki proje resimlerinde açık bir şekilde gösterilmeyecektir.
14. Velilerimizin iletişim bilgileri kendi bilgi ve istekleri haricinde asla 3. Şahıslarla paylaşılamaz.
15. 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. Bu eğitimler ders içi ve ders dışı olmak üzere Temel Eğitim Kurumları 1. ,2. , 3. , 4. Sınıf ders müfredatları konu ve kazanımlarına göre ilişkilendirilerek verilecektir.
16. Öğretmen ve öğrencilerimiz okulda sadece Milli Eğitim Bakanlığının denetimindeki internet ağını kullanabilirler.
17. Okulumuz internet ağına MEB SERTİFİKA güvenlik dosyası yüklenmeden internet ağına bağlanılamaz.
18. Okul içerisinde proje için bile olsa sadece öğretmenlerin kayıtlı cihazları kullanılır.
19. E-güvenlik politikamız Milli Eğitim Bakanlığı tarafından yayınlanan güvenli internet çerçevesine dâhildir. (Milli Eğitim Bakanlığı 2017/12 Sayılı Genelge)
20. Çalışanların tüm üyeleri, çocukları korumak için tek başına filtrelemeye güvenemeyeceklerinin farkındadır ve gözetim, sınıf yönetimi ve güvenli ve sorumlu kullanım eğitimi önemlidir.

21. Tüm okul ait cihazlar, okulun Kabul Edilebilir Kullanım Politikasına uygun olarak ve uygun güvenlik ve güvenlik önlemleri alınarak kullanılacaktır.
22. Personel üyeleri, web sitelerini, araçlarını ve uygulamalarını sınıfta kullanmadan önce veya evde kullanmayı önerirken daima değerlendirecektir.
23. Öğrenciler, bilginin konumlanması, alınması ve değerlendirilmesi becerileri de dahil olmak üzere, İnternette araştırmada etkili kullanımı konusunda eğitilecektir.
24. Okul, personelin ve öğrencilerin İnternet 'ten türetilen materyallerin telif hakkı yasalarına uygun olmasını ve bilgi kaynaklarını kabul etmesini sağlayacaktır.
25. Öğrencilere, okudukları ve ya gösterilen bilgilerin doğruluğunu kabul etmeden önce eleştirel düşünceleri öğretilecektir.

TÜM ÇALIŞANLARIN SORUMLULUKLARI ŞUNLARDIR:

1. Çevrimiçi güvenlik politikalarının geliştirilmesine katkıda bulunmak.
2. Kabul Edilebilir Kullanım Politikalarını (AUP 'lar) okumak ve onlara bağlı kalmak.
3. Okul sistemlerinin ve verilerin güvenliğinden sorumlu olmak.
4. Bir dizi farklı çevrimiçi güvenlik konusundaki farkındalığa sahip olmak ve onların bakımında çocuklarla nasıl ilişkili olabileceklerini bilmek.
5. Yeni ve gelişmekte olan teknolojiler kullanıldığında iyi uygulamaları modelleme.
6. Mümkün olduğunca müfredat ile çevrimiçi güvenlik eğitimini ilişkilendirme.
7. Okul koruma politikalarını ve prosedürlerini takip ederek endişe duyan bireylerin belirlenmesi ve uygun önlem alınması.
8. Olumlu öğrenme fırsatlarına vurgu yapmak.
9. Bu alanda mesleki gelişim için kişisel sorumluluk almak.
10. Öğrenci, veli, öğretmen ve diğer personel verilerini, şifre, bulut vb. yöntemlerle korumak.

ÇOCUK VE EBEVEYNLERE YÖNELİK e- GÜVENLİK ÖNLEMLERİ:

1. Aileye yönelik çocuk ve ergenlere denetimli, sınırlı ve amaçlı kullanım sağlayabilmeleri ile ilgili bilinçlendirme çalışmalarına devam edilmesine, öğrencilerimize cep telefonunun kullandırılmamasının önerilmesine, eğer kullanımı zorunluysa ebeveyn kontrol programı yüklenerek kullanılmasına;
2. İnternetin güvenli kullanımı ile ilgili paketlerin tanıtım ve yaygınlaşmasını sağlamak için projeler yapılmasına,
3. Evlerde internetin sınırlı kullanımını teşvik etmek için velilere ve ebeveynlere rehberlik yapılmaya devam edilmesine,
4. Kullanım farkındalığına yönelik uygulamalar geliştirmek için derslerde bu konuya öncelik verilmesine,
5. Ebeveynleri denetim yolları ve teknolojik imkânları ile ilgili bilinçlendirmek ve gerekli uygulamaları geliştirmek ve yaygınlaştırmak için üniversiteden akademisyenlerden yardım alınmasına, karar verilmiştir.

ÇOCUKLARIN BAŞLICA SORUMLULUKLARI ŞUNLARDIR:

1. Çevrimiçi güvenlik politikalarının geliştirilmesine katkıda bulunmak.
2. Okulun Kabul Edilebilir Kullanım Politikalarını okumak ve onlara bağlı kalmak.
3. Çevrimiçi ve çevrimdışı başkalarının hislerine ve haklarına saygı duymak.
4. İşler ters giderse, güvenilir bir yetışkinden yardım istemek ve çevrimiçi güvenlik sorunlarıyla karşılaşan diđer kişileri desteklemek.
5. Bireysel yaşlarına, yeteneklerine ve zayıf yönlerine uygun bir seviyede, kendilerini ve başkalarını çevrimiçi olarak korumak için sorumluluk almak.
6. Yeni ve gelişmekte olan teknolojilerin getirdiđi fırsatlar ve risklerle ilgili olarak kendi bilinci ve öğrenimlerinden sorumlu olmak.
7. Belli bir teknolojiyi kullanmanın kişisel risklerini deđerlendirmek ve bu riskleri sınırlamak için güvenli ve sorumluluk sahibi davranmak.
8. Okulda kullandığı, herkesin kullanımına açık cihazlarda, medya, bulut, mail vb. kişisel şifre ile koruduđu hesapları açık bırakmamak.
9. Güvenlik kameralarının okulda bulunma amacını öğrenmek.
10. Okulda, kişisel cihazlarından etkinliklerde izin alma harici, görüntü ve ses kaydı almamak.

EBEVEYNLERİN SORUMLULUKLARI ŞUNLARDIR:

1. Okul Kabul Edilebilir Kullanım Politikalarını okumak, çocuklarını bu politikaya bağlı kalmaya teşvik etmek ve uygun olduđunca kendilerinin de bağlı kalmasını sağlamak.
2. Çocuklarıyla çevrimiçi güvenlik konularını tartışmak, okulun çevrimiçi güvenlik yaklaşımlarını desteklemek ve evde uygun güvenli çevrimiçi davranışları pekiştirmek.
3. Teknoloji ve sosyal medyanın güvenli ve uygun kullanımını modellemek.
4. Davranışlarında, çocuđun çevrimiçi olarak zarar görme tehlikesi altında olduđunu gösteren deđişiklikleri belirlemek.
5. Okul veya diđer uygun kurumlardan, kendileri veya çocukları çevrimiçi problem veya sorunlarla karşılaşırse yardım veya destek istemek.
6. Okulun çevrimiçi güvenlik politikalarının oluşturulmasına katkıda bulunmak.
7. Öğrenme platformları ve diđer ađ kaynakları gibi okul sistemlerini güvenli ve uygun bir şekilde kullanmak.
8. Yeni ve gelişmekte olan teknolojilerin getirdiđi fırsatlar ve risklerle ilgili olarak kendi bilinci ve öğrenimlerinden sorumlu olmak.
9. Uzaktan çevrimiçi derslerde öğrencilerin derslere katılımı sırasında gerekli önlemleri almak.

OKUL/WEB SİTESİNİN YÖNETİLMESİ:

1. Web sitesinde iletişim bilgileri okul adresi, e-posta ve telefon numarası olacaktır. Personel veya öğrencilerin kişisel bilgileri yayınlanmayacaktır.
2. Okul Müdürü yayınlanan çevrimiçi içerik için genel yayın sorumluluđunu alacak ve bilgilerin dođru ve uygun olmasını sağlayacaktır.

3. Web sitesi, erişilebilirlik fikri mülkiyet haklarına saygı, gizlilik politikaları ve telif hakkı da dahil olmak üzere okulun yayın yönergelerine uyacaktır.
4. Spam maillerden korunmak için e-posta adresleri çevrimiçi olarak dikkatli bir şekilde yayınlanacaktır.
5. Öğrenci çalışmaları öğrencilerin izniyle ya da ebeveynlerinin izniyle yayınlanacaktır.
6. Web sitesinin yönetim hesabı uygun bir şekilde güçlü bir şifreyle korunacaktır.
7. Okul web sitemizde güvenli internet konulu bağlantılar mevcuttur.
8. Okul, çevrimiçi güvenlik dahil olmak üzere, toplumun üyeleri için okul web sitesinde korunma hakkında bilgi gönderecektir.

ÇEVİRİMİÇİ GÖRÜNTÜ VE VİDEOLAR YAYINLAMA:

1. Okulumuz, çevrimiçi paylaşılan tüm resimlerin ve videoların okul resim kullanımı politikasına uygun şekilde kullanılmasını sağlayacaktır.
2. Okulumuz , 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.
3. Görüntü politikasına uygun olarak, öğrencilerin resimlerinin / videolarının elektronik olarak yayınlanmasından önce her zaman ebeveynlerin yazılı izni alınacaktır.

CEP TELEFONU veya KAYDEDİCİ CİHAZLARIN KULLANIMI:

1. Öğrencilerimiz yaş itibari ile ilkökul seviyesinde oldukları için okula cep telefonu, tablet ve bilgisayar getirmeyeceklerdir.
2. Öğrenciler evde çevrimiçi canlı derslere katılırken cep telefonu, tablet veya bilgisayar kullanımı sırasında aileleri tarafından gerekli e-Güvenlik önlemleri alınacaktır. Sınıf Rehber Öğretmenleri tarafından öğrenciler ve aileleri alınması gereken e-Güvenlik önlemleri konusunda bilgilendirilecektir.
3. Öğrencilerimiz proje ve çalışmalar için okulun internet ve bilgisayarını kullanabilirler. Kullanım görevli öğretmenin kontrolünde e-güvenlik önlemleri alınarak filtrelemeler kontrol edilerek yaptırılır.

PERSONELİN CEP TELEFONU veya KAYDEDİCİ CİHAZLARININ KULLANIMI:

1. Öğretmenler ve yardımcı hizmetler personeli cep telefonlarını öğrencilerin bulunduğu zaman ve ortamlarda kullanamazlar.
2. Velilerle her yıl, eğitim öğretim yılı başında yapılan toplantıda cep telefonu kullanımı konusunda bilgi verilir.
3. Personel, kişisel telefonların ve cihazların herhangi bir şekilde kullanımının daima veri koruma ve ilgili okul politikası ve prosedürleri uyarınca yerine getirilmesini sağlayacaktır
4. Personel kişisel cep telefonları ve cihazları ders saatlerinde kapatılıp / sessiz moda geçirilir.
5. Bluetooth veya diğer iletişim biçimleri ders saatlerinde "gizlenmiş" veya kapalı olmalıdır.
6. Bir personel okul politikasını ihlal ettiği durumlarda disiplin işlemi yapılır.

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

ZİYARETÇİ KİŞİSEL CİHAZLAR VE CEP TELEFONLARININ KULLANIMI:

1. Ebeveynler ve ziyaretçiler, okulun kabul edilebilir kullanım politikasına uygun olarak cep telefonlarını ve kişisel cihazları kullanmalıdır.
2. Fotoğraflar veya videolar çekmek için ziyaretçiler ve ebeveynler tarafından cep telefonlarının veya kişisel cihazların kullanılması, okul resim kullanım politikasına uygun olarak gerçekleştirilmelidir.
3. Okul, ziyaretçilere kullanım beklentilerini bildirmek için uygun tabela ve bilgileri sağlayacak ve sunacaktır.
4. Personelin uygun ve güvenli olduğunda sorunlara karşı çıkması beklenir ve her zaman ziyaretçilerin herhangi bir ihlalini idareye bildirecektir.
5. Ziyaretçilerin ve ebeveynlerin okul içerisinde öğrencilere yönelik fotoğraf veya video çekmesi kabul edilemez. Bu nedenle gerekli uyarılar yapılır.
6. Okul idaresi tarafından görevli kılınanlar haricindeki kişiler tarafından ve öğrenci velilerinin bilmek istedikleri etkinlik ve programlar dışındaki zamanlarda, okul ve okul bahçesi sınırları içerisinde fotoğraf ve video çekimi yapılamaz. Bu yasak bir öğrencinin diğer bir öğrencinin fotoğraf ve videosunu çekmek istemesi durumunda da geçerlidir.
7. Okul idaresi tarafından görevlendirilen kişilerin çektiği fotoğraf ve videolar ancak Okulun resmi web adresinde ve sanal ortamlarında, ilgili öğrenci velisinin talep ve yazılı onayı ile yayınlanabilir. Öğrencisi için onay vermeyen velinin öğrencisi ile ilgili fotoğraf ve videolar yayınlanmaz.
8. Velisi tarafından fotoğraf ve video görüntülerinin çekilip yayınlanmasına onay verilmeyen öğrencilerin, çekim esnasında psikolojik baskı yaşamaması için tedbirler alınır.
9. Okul görevlileri tarafından yayınlanan resim ve videolarda öğrencilerin kişisel bilgilerine kesinlikle yer verilmez.
10. Online dersler kapalı bir sistem üzerinden yalnızca okula kayıtlı öğrenciler ile yapılabilir.

OKUL PERSONELİNE YÖNELİK GÜVENLİK ÖNLEMLERİ:

1. 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 sağlanmasına,

2.Çalışanların hepsi, çevrimiçi davranışlarının okuldaki rolü ve itibarını etkileyebileceğinin farkına varacaktır. Mesleği veya kurumu tehlikeli durumuna düşürdüğü veya mesleki yeteneklerine güvenini kaybetmiş bir şeyin bulunduğu düşünülürse, hukuk, disiplin veya hukuki önlemler alınabileceğinin tebliğ edilmesine.

3.Okul çalışanların öğrencilerin yaşlarına ve yeteneklerine göre kullanması gereken yararlı çevrimiçi araçları kontrol etmelidir. Sınıflardaki akıllı tahtaların teneffüslerde açık kalmamasına dikkat etmelidirler. Çocukların internetin ve dijital teknolojinin güvenilir ve sorumlu kullanıcıları olabilmesi için ana-babanın / bakıcıların oynayacakları önemli bir role sahip olduklarını kabul eder.

ÇOCUKLARIN KATILIMI VE EĞİTİMİ:

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

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

3.Tüm kullanıcılara ağ ve internet kullanımının izleneceği bildirilecektir.

4.Kabul Edilebilir Kullanım beklentileri ve Posterler, İnternet erişimi olan tüm odalarda yayınlanacaktır. Panolar hazırlanacaktır.

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

6.Okul, öğrencilerin teknolojiyi olumlu şekilde kullandıklarını ödüllendirecektir.

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

8. Okulumuzda Güvenli İnternet Günü kutlanmaktadır.

Güvenli İnternet Günü çerçevesinde şubat ayının ilk haftasında sınıflarda sunumlar yapılır videolar izletilir. Ayrıca Şubat ayı veli toplantılarına yer verilir.

PERSONELİN KATILIMI VE EĞİTİMİ:

1.Çevrimiçi güvenlik (e-Güvenlik) politikası, tüm çalışanların katılımı için resmi olarak sağlanacak ve tartışılacak ve korunma sorumluluğumuzun bir parçası olarak güçlendirilecek ve vurgulanacaktır.

2. Okulumuz Personeli yıl içinde yapılan öğretmenler kurulu toplantılarında okulumuz e-güvenlik politikası hakkında bilgilendirilecek. Görüş alış verişinde bulunularak e-güvenlik politikası geliştirilecek.

3.Okulumuzda aynı sınıf okutan öğretmenler arasında yapılan zümre öğretmenler kurulu toplantılarında okulumuzun e-güvenlik politikası gündeme alınarak görüşülecektir.

4.Personel, İnternet trafiğinin izlenebileceğini ve tek bir kullanıcıya kadar izlenebileceğinin farkında olacak. Okul sistemlerini ve cihazlarını kullanırken takdir yetkisi ve profesyonel davranış gereklidir.

5.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.

EBEVEYNLERİN KATILIMI VE EĞİTİMİ:

1. Dede Korkut İlkokulu, çocukların internetin ve dijital teknolojinin güvenilir ve sorumlu kullanıcıları olabilmesi için ana-babaların oynayacakları önemli bir role sahip olduklarını kabul eder.
2. Ebeveynlerin dikkatleri, okul açıklamaları ve okul web sitesinde okul çevrimiçi güvenlik (e-Güvenlik) politikasına ve beklentilerine yönelecektir.
3. Çevrimiçi güvenlik konusundaki ebeveynler için bilgi ve rehberlik, ebeveynlere çeşitli biçimlerde sunulacaktır. E-güvenlik veli bilgilendirme toplantıları yapılacak ayrıca okul genel veli toplantıları, sınıf veli toplantılarında e-güvenlik gündem maddesi olarak alınarak gerekli bilgilendirme ve görüş alışverişinde bulunulacaktır.
4. Ebeveynlerin, e-güvenlik kapsamında çocukları için olumlu davranışları rol modellemeleri teşvik edilecektir.

ÇEVİRİMİÇİ OLAYLARA VE KORUMA SORUNLARINA YANIT VERME:

1. Okulun 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.
2. Okulun tüm üyeleri, filtreleme, cinsel içerikli mesajlaşma, siber zorbalık, yasadışı içerik ihlali vb. gibi çevrimiçi güvenlik (e-Güvenlik) endişelerini bildirme prosedürü hakkında bilgilendirilecektir.
3. Dijital Abone Hattı (DSL), daha sonra kaydedilecek olan çocuk koruma endişelerini içeren herhangi bir çevrimiçi güvenlik (e-Güvenlik) olayı hakkında bilgilendirilecektir.
4. İnternet'in yanlış kullanımı ile ilgili şikayetler, okulun şikayet prosedürleri kapsamında ele alınacaktır.
5. Çevrimiçi / siber zorbalık ile ilgili şikayetler, okulun zorbalık karşıtı politikası ve prosedürü kapsamında ele alınacaktır.
6. Personelin yanlış kullanımı ile ilgili herhangi bir şikayet okul müdürüne yönlendirilecektir.
7. Okul şikayet prosedürü öğrencilere, velilere ve personele bildirilecektir.
8. Şikayet ve ihbar prosedürü personele bildirilecektir.
9. Okulun tüm üyeleri, gizliliğin öneminden ve endişeleri bildirmek için resmi okul usullerine uyma ihtiyacından haberdar olmalıdırlar.

10. Okulun tüm üyeleri, çevrimiçi ortamda güvenli ve uygun davranış hakkında hatırlatılacak ve okul camiasının herhangi bir diğer üyesine zarar vermek, sıkıntı yaşamak veya suç oluşturan herhangi bir içerik, yorum, resim veya video yayımlamamanın önemini hatırlatacaktır.
11. Okul, çevrimiçi güvenlik (e-Güvenlik) olaylarını, uygun olduğunda, okul disiplini / davranış politikasına uygun olarak yönetir.
12. Okul, ebeveynlere, ihtiyaç duyulduğunda bunlarla ilgili endişeleri bildirir.
13. Herhangi bir soruşturma tamamlandıktan sonra okul bilgi alacak, öğrenilen dersleri belirleyecek ve değişiklikleri gerektiği gibi uygulayacaktır.
14. Sorunları çözmek için ebeveynlerin ve çocukların okulla ortak çalışması gerekir.

GÖZDEN GEÇİRME :

Bu dokümanı gözden geçirme her yıl Haziran ayında yapılır. Yapılan değişiklik ve güncellemeler İdare onayıyla yayınlanır.

OKUL e-TWİNNİNG ve e-GÜVENLİK EKİBİ

Aysun YÜCEL YURDAY (Sınıf Öğretmeni)

Nazmiye SUBASAR (Sınıf Öğretmeni)

Selma KARA (Sınıf Öğretmeni)

Zehra YILMAZ (İngilizce Öğretmeni)

Derya UYAN (Rehber Öğretmen)

Seçil OLGUN (Sorumlu Müdür Yardımcısı)

İbrahim ŞEN (Sorumlu Müdür Yardımcısı)

Feyyaz DEMİRBAŞ (Okul Müdürü)