**KARAPINAR TİCARET BORSASI İLKOKULU**

 **E-GÜVENLİK POLİTİKASI**

Ticaret Borsası İlkokulu Konya’nın Karapınar ilçesi merkez Adalet Mahallesi’ nde yer almaktadır. Kurumumuz 7176 metre karelik alana 2000 yılında kurulmuştur. Okulumuz “Eğitimde kalite ve başarıları ile fark yaratan bir kurum olma” vizyonu ile yola çıkmış, “Mutlu, özgüvenli, başarılı, ilkeli, açık fikirli, araştıran-sorgulayan, iletişim becerileri gelişmiş, öğrenmeye ve yeniliklere açık, öz değerlendirme yapabilen, işbirliğine yatkın, yaratıcı ve eleştirel düşünen, akılcı, cesaretli, çok yönlü, gelişime açık, ulusal kültürünü özümsemiş, aynı zamanda kültürel bakış açısına sahip bireyler yetiştirme” misyonuna sahip bir kurumdur.

 **Tüm çalışanların sorumlulukları şunlardır:**

• Çevrimiçi güvenlik politikalarının geliştirilmesine katkıda bulunmak.

• Okul e-güvenlik politikalarını okumak ve onlara bağlı kalmak.

• Okul 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 modellemek.

• 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.

 **Öğrencilerin başlıca sorumlulukları şunlardır:**

• Çevrimiçi güvenlik politikalarının geliştirilmesine katkıda bulunmak.

• Okul e-güvenlik politikalarını okumak ve onlara bağlı kalmak.

• Çevrim içi ve çevrimdışı 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 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.

**Ebeveynlerin başlıca sorumlulukları şunlardır:**

• Okul e-güvenlik politikalarını okumak , çocuklarını bu politikaya bağlı kalmaya teşvik etmek ve uygun olduğunca kendilerinin de bağlı kalmasını sağlamak.

• Çocuklarıyla çevrimiçi güvenlik konularını tartışmak, okulun çevrimiçi güvenlik yaklaşımlarını desteklemek ve evde uygun güvenli çevrimiçi davranışları pekiştirmek.

• Teknoloji ve sosyal medyanın güvenli ve uygun kullanımını modellemek.

• Davranışlarında, çocuğun çevrimiçi olarak zarar görme tehlikesi altında olduğunu gösteren değişiklikleri belirlemek.

• Okul veya diğer uygun kurumlardan, kendileri ve ya çocukları çevrimiçi problem veya sorunlarla karşılaşırsa yardım veya destek istemek.

• Okulun çevrimiçi güvenlik politikalarının oluşturulmasına katkıda bulunmak.

• Öğrenme platformları ve diğer ağ kaynakları gibi okul sistemlerini güvenli ve uygun bir şekilde kullanmak.

• Yeni ve gelişmekte olan teknolojilerin getirdiği fırsatlar ve risklerle ilgili olarak kendi bilinci ve öğrenimlerinden sorumlu olmak.

**Okul Web Sitesinin Yönetilmesi**

Okulumuza ait web sitesi kullanımında Milli Eğitim Bakanlığı’nın [**05/06/2018 tarih ve 10943576 sayılı Okul İnternet Siteleri Yönergesi**](http://mevzuat.meb.gov.tr/dosyalar/1958.pdf)hükümleri gereğince hareket edilmektedir. İlgili yönergede;

MADDE 8 – (1) Kullanıcı Yönetimi: İnternet sitesi yayın ekibi yöneticisi, kurum MEBBİS kullanıcı adı ve şifresi ile panele giriş yaparak internet sitesi yayın ekibi kullanıcı hesaplarını oluşturur. İnternet sitesi yayın ekibinden ayrılan veya internet sitesi yayın ekibine katılan kişilerin kullanıcı hesapları internet sitesi yayın ekibi yöneticisi tarafından güncellenir.

 (2) Panelde yer alan, kuruma ait temel bilgilerin veri girişi yapılır.

(4) İçerik; hedef kitleye yönelik güncel, zengin ve tutarlı olur.

(5) Okul internet sitelerinde yayınlanacak içerikler: internet sitesinin etkin ve verimli kullanımını sağlamak amacıyla okul tanıtımı, öğrencilerin çeşitli alanlardaki proje çalışmaları, kültürel, sanatsal ve sportif faaliyetleri, öğretmenlerin hazırladıkları özgün eğitim içerikleri, rehberlik çalışmaları ve benzeri içerikleri kapsar.

(6) Oluşturulan içerikler, internet sitesi ziyaretçilerinin kurum hakkında olumlu bir algıya sahip olmalarına ve güven duygusunun oluşmasına, hedef kitlenin aidiyetlerinin artmasına yardımcı olacak nitelikte olur.

 (7) Haber kategorisindeki içerikler; ne, nerede, ne zaman, nasıl, niçin, kim (5N 1K) sorularına cevap verecek şekilde hazırlanır. Haberler, kurumla doğrudan ilgili ve kurumsal kimliğe zarar vermeyecek nitelikte olur. (13)Kişisel verilerin korunması kapsamında; internet sitesinde kişiyi tam olarak belirlenebilir kılan (T.C. Kimlik No, anne-baba adı, iletişim ve ikametgâh bilgileri ve benzeri) bilgilerin yer aldığı listeler yayınlanmaz.

(14)Okul internet sitesinde yönetici, öğretmen, diğer personel ve öğrencilere ait görsellerin yayınlanabilmesi için ilgiliden muvafakatname alınır. Okul internet sitesinde kullanılacak her türlü görsel bu muvafakatname esas alınarak seçilir.

(15)Hakkında koruma kararı bulunan öğrencilere ait bilgi ve fotoğraflar hiçbir surette yayınlanmaz.

(16)İnternet sitesinde, öğrenciler için eğitici niteliği olmayan, pedagojik açıdan sakıncalı içerik, bağlantı ve medya (oyun, video, uygulama ve benzeri) yayınlanmaz.

(17)Okul /kurum internet sitelerinde reklam yayınlanmaz.

18) 6698 Sayılı Kişisel Verilerin Korunması Kanunu kapsamında, yayınlanacak her türlü içerik telif hakları, fikri haklar, şeref ve haysiyetin korunması ve gizlilikle uyumlu olur. Bakanlığın herhangi bir politikasını, kuralını ya da düzenlemesini ihlal edemez. Mevzuatla belirlenen hususlara aykırı olmaz.

(19)Panel Yetkilisi,

a) Panelde yer alan bilgilere zarar vermez; işleyişi aksatma, yavaşlatma veya durdurma eylemlerinde bulunmaz, içeriğini yetkisiz olarak değiştirmez.

b) Kendi kullanıcı bilgilerini; kimseyle paylaşmaz; bu bilgileri başkasının kullanımına izin vermez.

c) Bilgi teknolojileri kapsamında, panelde yer alan herhangi bir kaynağı, hiç kimse adına ve yararına kullanmaz.

 ç) Diğer panel yetkililerinin hesap bilgilerini kullanarak yetki gerektiren alanlara erişmez.

 d) İnternet sitesinin çalışmasını etkileyen arızaları mümkün olan en kısa sürede uygun iletişim kanallarını kullanarak Başkanlığa rapor eder.

e) Panelde yer alan gizlilik gerektiren bilgileri, kişisel veriler ve veri içeren ekran görüntülerini paylaşmaz.

Güvenlik politikası MADDE 10 – (1) Başkanlığın onayı olmadan Bakanlık sunucuları haricinde internet sitesi ve veri tabanı barındırılmaz.

(2) Herhangi bir siber saldırı halinde işlem yapılmadan, tespit edilen sorunlar Başkanlığa bildirilir. (3) Tahsis edilen internet sitesi alanına virüs ve benzeri zararlı içerikler ile yetkisiz erişime neden olabilecek uygulamalar yüklenmez.

(4) İnternet sitesi barındırma alanı internet sitesi yayıncılığı dışında dosya depolama veya arşiv alanı olarak kullanılmaz.

**Çevrimiçi görüntü ve videolar yayınlama**

• Okul, çevrimiçi paylaşılan tüm resimlerin ve videoların , Milli Eğitim Bakanlığı tarafından yayınlanan **07/03/2017 tarih ve 2975829 sayılı 2017/12 Okullarda Sosyal Medyanın Kullanılması Genelgesi**’ne uygun şekilde kullanılmasını sağlayacaktır. <http://mevzuat.meb.gov.tr/dosyalar/1833.pdf>

• Okul , resimlerin ve videoların tümünün, veri güvenliği, Okul e-Güvenlik 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.

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

• 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 cevaplamaya ayarlanmayacaktır.

• Harici IP adresleri diğer 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.

**Kullanıcılar**

• 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 tutulacak.

**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.

• Okul, bir video konferansa katılmadan önce diğer konferans katılımcılarıyla diyalog kuracak. Okul değilse, okul sınıf için uygun olan materyali teslim aldığını kontrol edecektir.

**İnternetin ve ilgili cihazların uygun ve güvenli kullanımı**

Okul yönetimi;

* Güvenlik açıklarını önlemek için güvenlik duvarlarının ve anti-virüs koruma sistemlerinin yüklenmesi ve bunların güncel tutulması
* Okuldaki makinelerde kullanılan web tarayıcılarının güvenlik ayarlarının kişiselleştirilerek istenmeyen web sitelerinin ve pop-up'ların engellenmesinden sorumludur.
* Öğrencilere bunların neden yapıldığının anlatılacak ve yapılanların onları korumaya yönelik olduğu açıklanacaktır.
* İnternetin kullanımı ve okuldaki makinelerde kişisel postaların kötü amaçlı yazılımlara karşı otomatik olarak denetimi konusunda kurallarla ilgili tüm ilgililer bilgilendirilecektir.
* Kullanıcılara, dosya indirirken veya taşınabilir cihazlar kullanırken potansiyel olarak virüs bulaşmış dosyaları ve güvenli uygulamaları tespit etmeleri için temel eğitimler verilecektir.
* Personel ve öğrenciler dahil olmak üzere herkese, okul makinelerinde kullanmadan önce tüm dosyalara kötü amaçlı yazılım taraması yapmaları gerektiği öğretilecektir.
* Kötü amaçlı yazılımlarla ilgili tüm sorunları ele almak ve resmi bir olay işleme prosedürünü yerine getirmek için eğitimli bir kişi (Formatör Bilişim Teknlojileri Öğretmeni) belirlenecektir..
* Tüm çevrimiçi toplulukların bazen “topluluk yönergeleri” olarak da adlandırılan kendi davranış kuralları bulunmaktadır. Örneğin, eTwinning’te, tüm kayıtlı kullanıcılar için geçerli olan Davranış Kuralları mevcuttur. Davranış Kuralları ile ilgili bilgilendirmeler yapılacaktır.

 Faydalı kaynaklar:

**1**. eTwinning’in kendine ait internet görgü kuralları bulunmaktadır. eTwinning Portalına göz atın. Söz konusu kuralllara [buradan](https://www.etwinning.net/en/pub/code-of-conduct.htm) ulaşabilirsiniz.
**2.** Günümüzdeki en popüler çevrimiçi toplulukların bazılarında uygulanan kılavuzlara ve davranış kurallarına göz atın:
**a.**[**Facebook**](https://www.facebook.com/communitystandards)
**b. [YouTube](http://www.youtube.com/yt/policyandsafety/communityguidelines.html%22%20%5Ct%20%22_blank)**
**c.** **[Twitter](https://support.twitter.com/articles/87137%22%20%5Ct%20%22_blank)**
**d.** **[Instagram](https://help.instagram.com/477434105621119/%22%20%5Ct%20%22_blank)**
**e. [Snapchat](https://support.snapchat.com/en-US/a/guidelines%22%20%5Ct%20%22_blank)**
**3.**Ayrıca [Kent County Council](https://www.kelsi.org.uk/__data/assets/pdf_file/0008/73835/Complaints-on-Social-Networking-Sites.pdf) adlı araştırmaya bakın.
**4.** Bunların yanı sıra; çocuklar ve gençler (ve yetişkinler) tarafından yaygın bir şekilde kullanılan en popüler uygulamalar, sosyal ağ siteleri ve diğer platfomlar hakkında önemli bilgiler sunmayı amaçlayan [Better Internet for Kids guide to online services (Çocuklar için daha iyi bir İnternet)](https://www.betterinternetforkids.eu/web/portal/onlineservices%22%20%5Ct%20%22_blank) web sitesini ziyaret edin.

* Milli Eğitim Bakanlığı ile Bilgi Teknolojileri ve İletişim Kurumu arasında imzalanan **21 Mayıs 2012 tarihli Protokol. ve 28.08.2013 tarih ve 30706984/774/2237778** sayılı yazı. FATİH Projesi kapsamında bilişim teknolojilerinin ve intemetin bilinçli, güvenli kullanımı konusunda öğrenci, öğretmen ve ebeveynlerde farkındalığın arttırılması amacıyla protokol imzalanınıştır. Protokol doğrultusunda öğretmenlerimizin FATİH Projesi Bilişim Teknolojilerinin ve İnternetin Bilinçli, Güvenli Kullanımı Seminerlerine katılarak sertifikalarını almaları sağlanacaktır.
* Öğrencilerimize internetin bilinçli ve güvenli kullanımı ile ilgili seminerler düzenlenecektir. <http://www.meb.gov.tr/duyurular/duyurular2011/guvenliinternet/>

<http://kticaretborsaio.meb.k12.tr/icerikler/guvenli-internet-kullanimi_8694042.html>

**Öğrencilerin kişisel cihazlar ve cep telefonları kullanımı**

• 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 telefonuyla çocuklarıyla iletişim kurmamaları, okul idaresine başvurmaları önerilir. İstisnai durumlarda öğretmenin onayladığı şekilde istisnalara izin verilebilir.

• Öğrenciler, telefon numaralarını yalnızca güvenilir arkadaşlarına ve aile üyelerine vermelidirler.

• Öğrencilere, cep telefonlarının ve kişisel cihazların güvenli ve uygun bir şekilde kullanımı öğretilecek ve sınırların ve sonuçların farkına varılacaktır.

* Bir cep telefonuna el konulması durumunda; telefondaki kişisel verilerin korunmasını sağlamak amacıyla, öğrenci telefonu öğretmene teslim etmeden önce kapatmalıdır. Eğer telefon okul gününün sonunda geri verilmezse, veliler bilgilendirilmeli ve cep telefonu güvenli bir yerde saklanmalıdır.

**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 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 ulaşılacaktır.

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

**Çocukların eğitimi**

• Öğrenciler arasında güvenli ve sorumlu internet kullanımının önemi ile ilgili farkındalık yaratmak için bir çevrimiçi güvenlik (e-Güvenlik) müfredatı oluşturulur ve okulun tamamında yer alır.

• Güvenli ve sorumlu kullanım ile ilgili eğitim internet erişiminden önce yapılacaktır.

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

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

• Tüm kullanıcılara ağ ve internet kullanımının izleneceği bildirilecektir.

• Çevrimiçi güvenlik (e-Güvenlik) BİT programlarına dahil edilecek ve hem güvenli okul hem de evde kullanımını kapsayacaktır.

• Okul e-Güvenlik Politikası ve Posterler, Internet erişimi olan tüm odalarda yayınlanacaktır.

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

• Dışarıdan destek, okulların dahili çevrimiçi güvenlik (e-Güvenlik) eğitim yaklaşımlarını tamamlamak ve desteklemek için kullanılacaktır.

• Okul, öğrencilerin teknolojiyi olumlu şekilde kullandıklarını ödüllendirecektir.

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

**Personelin eğitimi**

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

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

Personelin tüm üyelerine, profesyonel ve kişisel olarak, güvenli ve sorumlu İnternet kullanımı konusunda güncel ve uygun personel eğitimi, düzenli (en az yıllık) temelde çeşitli şekillerde sağlanacaktır.

• Çalışanların tüm üyeleri, çevrimiçi davranışlarının okuldaki rolü ve itibarını etkileyebileceğinin farkına varacaktır. Mesleği veya kurumu çürüme durumuna düşürdüğü veya profesyonel yeteneklerine güvenini kaybetmiş bir şeyin bulunduğu düşünülürse, kamusal, disiplin veya hukuki önlemler alınabilir.

• Filtreleme sistemlerini yönetme veya BİT kullanımını izleme sorumluluğu taşıyan personelin üyeleri, Liderlik Ekibi tarafından denetlenecek ve sorunları veya endişeleri bildirmek için açık prosedürlere sahip olacaklar.

• Okul, çalışanların öğrencilerin yaşlarına ve yeteneklerine göre kullanması gereken yararlı çevrimiçi araçları vurgulamaktadır.

**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. 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 şikayetler, okulun şikayet prosedürleri kapsamında ele alınacaktır.

• Çevrimiçi / siber zorbalık ile ilgili şikayetler, okulun zorbalık karşıtı politikası ve prosedürü kapsamında ele alınacak

• Personelin yanlış kullanımı ile ilgili herhangi bir şikayet okul müdürüne yönlendirilecektir

• Okul şikayet prosedürü öğrencilere, velilere ve personele bildirilecektir.

• Şikayet ve ihbar prosedürü personele bildirilecektir.

Okulun tüm üyeleri, gizliliğin öneminden ve endişeleri bildirmek için resmi okul usullerine uyma ihtiyacından haberdar olmalıdırlar.

• Okulun tüm üyeleri, çevrimiçi ortamda güvenli ve uygun davranış hakkında hatırlatılacak ve okul camiasının herhangi bir diğer üyesine zarar vermek, sıkıntı yaşamak veya suç oluşturan herhangi bir içerik, yorum, resim veya video 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.