AŞAĞIBAĞLAR ANAOKULU
E-GÜVENLİK POLİTİKASI

Giriş

Teknolojinin günlük hayattaki yeri ve önemi günden güne artmakta ve hayatın vazgeçilmez bir bütünü olmaktadır. İnsan hayatına günden güne daha fazla yerleşen teknoloji ve internetin kullanım alanı oldukça genişlemiştir. Her gün daha da fazla gelişen teknoloji ve daha da genişleyen internet kullanım alanı bireyleri olumlu yönde etkilediği gibi beraberinde getirdiği birçok tehlikeye karşı savunmasız bırakabilmektedir. Her gün gelişen teknoloji ve internet kullanım alanının sınırları o kadar genişlemiştir ki denetim altına almak çok zor hale gelmiştir. Teknolojinin bilinçsiz ve güvensiz kullanımı bireylerin birçok şekilde mağduriyetine neden olmaktadır. Bunlardan bir kaçını şu şekilde sıralayabiliriz.

1. Bilgisayar Sistemlerine ve Servislerine Yetkisiz Erişim
2. Bilgisayar Sabotajı
3. Bilgisayar Yoluyla Dolandırıcılık
4. Bilgisayar Yoluyla Sahtecilik

5. Bir Bilgisayar Yazılımının İzinsiz Kullanımı

6. Kişisel Verilerin Kötüye Kullanılması

7. Sahte Kişilik Oluşturma ve Kişilik Taklidi

8. Yasadışı Yayınlar

9. Ticari Sırların Çalınması

10. Terörist Faaliyetler

11. Çocuk Pornografisi

12. Hacking

13. Diğer Suçlar (Organ, fuhuş, tehdit, uyuşturucu, vb.)

Hayatımızı son derece kolaylaştıran ve birçok noktada hayatımıza olumlu dokunuşları olan teknoloji ve internet kullanımının bilinçsiz ve ya bilinçli bir şekilde kötüye kullanımı söz konusu olabilmektedir. İnsanların teknoloji ve internet ortamında ki mağduriyetleri nedeni ile kişisel, sosyal, psikolojik, ekonomik, ahlaki, manevi çöküntüler yaşamakta ve toplum sağlığı tehlikeye girmektedir. Bu ve buna benzer birçok sorun ile karşılaşmamak, idarecilerimizin, öğretmenlerimizin, öğrencilerimizin, velilerimizin ve okul personelimizin bilinçli bir kullanıcı olmaları adına Aşağıbağlar Anaokulu olarak E-Güvenlik Okul politikasını oluşturmayı gerekli bulmuştur.

Amaç ve Kapsam

Bu politikanın amacı Aşağıbağlar Anaokulunda görev yapan Okul İdaresi, Öğretmenler, Okul Personelini ve Okula kayıtlı olan Öğrenci ve velilerini güvenli teknoloji ve internet kullanımı konusunda bilinçlendirmek ayrıca okulda ve evde bulundukları süre zarfında teknoloji ve internet kullanımı konusunda güvende olmalarını sağlamaktır. Bu nedenle okuldaki tüm teknolojik aletler ve kişisel cihazlar bu politika kuralları ve denetimine tabiidir.

Dayanak

Türk Ceza Kanunu 244. madde ile bir bilişim sisteminin işleyişini engelleyen veya bozan bir kişi bir yıldan beş yıla kadar hapis cezası ile cezalandırılır hükmü ile bir bilişim sistemindeki verileri bozan, yok eden, değiştiren veya erişilmez kılan, sisteme veri yerleştiren var olan verileri başka bir yere gönderen kişi altı aydan üç yıla kadar hapis cezası ile cezalandırılır hükmü getirilmiştir. 245. madde ile de banka ve kredi kartlarının kötüye kullanılması eylemleri bağımsız bir suç tipi olarak düzenlenmiştir. Kredi kartı veya banka kartıyla gerçekleştirilen her türkü hukuka aykırı yarar sağlama eylemi bu suç tipini

oluşturmaktadır. Bilişim suçları yanı sıra internet içerik düzememelerine birden fazla kanunda yer verilmekle birlikte bunlardan en önemlisi olan 5651 sayılı "İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun" 2007 yılında yürürlüğe girmiştir. Kanun ile ilk defa internet ortamındaki katalog suçlar kapsamındaki yasadışı içerik ile ilgili erişimin engellenmesi usul ve esasları düzenlenmiş ve internet hizmeti veren internet aktörlerine de bir takım yükümlülük ve sorumluluklar getirilmiştir. Kanunda tanımlanmış katalog suçlara ilişkin; Bilgi Teknolojileri ve İletişim Kurumu Bilgi ve İhbar Merkezi; vatandaşların bu suçlara ilişkin şikâyetlerini bildirebilecekleri müracaat merkezi olarak kurulmuştur. 23.11.2007 tarihinde faaliyete geçen bu merkeze http://www.ihbarweb.org.tr adlı web adresinden yasadışı içeriğe ilişkin ihbarda bulunabilmektedir. Kanun kapsamında ayrıca vatandaşlara internet ortamında kişilik haklarının ihlali ve özel hayatın gizliliği ile ilgili olarak başvuru süreçleri tanımlanmıştır.
6698 Sayılı Kanun-Kişisel Verilerin Korunması Kanunu Madde 5:Kişisel Veriler ilgili kişinin açık rızası olmaksızın işlenemez. Madde 8: Kişisel Veriler ilgili kişinin açık rızası olmaksızın aktarılamaz.
Okul İdaresi, Öğretmen ve Okul personeli sorumlulukları;
* Tüm çalışanlar politikaya uymak ve uygulanmasını
* E – Güvenlik politikasının geliştirilmesi, uygulanabilir diğer politikaların takibini yapılması, okula entegre edilmesi
* Okuldaki teknolojik aletlerin ve internetin güvenli şekilde kullanılmasın. Bu kapsamda okuldaki tüm bilgisayarlara anti-virüs sistemi yüklenmiş, kullanıcı hesapları oluşturulmuş, şifreler tanımlanmıştır. Ayrıca Milli Eğitim Bakanlığı Güvenlik Sertifikası tüm bilgisayarlara yüklenerek internet erişimi güvenli hale getirilmiştir.
Bunun yanı sıra internette ki kötü amaçlı saldırı ve ihlalleri engellemek adına ağ güvenliği için gerekli programlar ve güvenlik durumları aktif hale getirilmiştir.
Ürünler lisanslı şekilde kullanılıp sahte ve korsan program ve ürünlere kesinlikle yer verilmemiştir.
* Okuldaki sistem ve verilerin korunmasından sorumlu olmak
* Çevrimiçi güvenlik konusunda bilgi sahibi olmak ve bunu öğrencilere yıl boyunca entegre etmek
* Yeni gelişme ve güncelleri takip etmek
* Teknolojik alet ve internet kullanımı ile ilgili olumsuzlukları tespit etmek ve önüne

geçmek

* Müfredat ile E-Güvenliği ilişkilendirmek

* Gelişen ve değişen teknolojiler doğrultusunda E-güvenliği güncellemek

Öğrencilerin Sorumlulukları;

* Okul Öncesi düzeydeki öğrencilerin sorumluluğu E-Güvenliğin geliştirilmesine katkıda bulunmak

* Herhangi bir sorun ile karşılaştığında öğretmenleri veya aile üyelerinden yardım alabileceğini bilmek

* Özel Alan bilinci ve özel alana saygılı olma,

* Başka insanların haklarının farkında olma ve bu haklara saygı duyma

* Başkalarının his ve duygularını anlayabilme, Empatik düşünebilme

* Teknolojinin insan hayatına olumsuz etki edebileceğinin farkında olması

Ebeveynlerin Başlıca Sorumlulukları;

* 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 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

* 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 sorumluluğunu alacak ve bilgilerin doğru ve uygun olmasını sağlayacaktır.

* Web sitesi, erişilebilirlik fikri mülkiyet haklarına saygı, gizlilik politikaları ve telif hakkı da dahil olmak üzere 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 dahil olmak üzere, toplumun üyeleri için okul web sitesinde korunma hakkında bilgi gönderecektir.

Çevrimiçi görüntü ve videolar yayınlama

* 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 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.

Kullanıcılar

* 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

* 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 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.
* 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 okula kayıtlı cihazları kullanılır.
* Diğer proje partnerleri ile iletişim ve görüntülü iletişim öğretmenler tarafından okul saatlerinde yapılmaktadır.
* 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.
* Personel üyeleri, web sitelerini, araçlarını ve uygulamalarını sınıfta kullanmadan önce veya evde kullanmayı önerirken daima değerlendirecektir.
* Okul, personelin ve öğrencilerin İnternet´ten türetilen materyallerin telif hakkı yasalarına uygun olmasını ve bilgi kaynaklarını kabul etmesini sağlayacaktır.
* Öğrencilere, öğrendikleri veya gösterilen bilgilerin doğruluğunu kabul etmeden önce eleştirel düşünmeleri öğretilecektir.

Kişisel Cihazların ve Cep Telefonlarının Kullanımı

* Cep telefonlarının ve çocukların, gençlerin ve yetişkinler arasındaki diğer kişisel cihazların yaygın bir şekilde sahiplenilmesi, tüm üyelerin Aşağıbağlar Anaokulu 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 dahil olmak üzere uygun politikalarda yer alacaktır.
* 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.

Kişisel cihazların ve cep telefonlarının güvenli bir şekilde kullanılması için beklentiler

* 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.
* Aşağıbağlar Anaokulu topluluğunun tüm üyelerine cep telefonlarını veya cihazlarını kayıp, hırsızlık veya hasardan korumak için adım atmaları önerilir.
* Aşağıbağlar Anaokulu 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.
* Aşağıbağlar Anaokulu 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.

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.

Ziyaretçiler kişisel cihazların ve cep telefonlarının kullanılması

* 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.

Çocukların ve gençlerin katılımı ve eğitimi

* Öğrenciler arasında güvenli ve sorumlu internet kullanımının önemi ile ilgili farkındalık yaratmak için bir çevrimiçi güvenlik (e-Güvenlik) müfredatı oluşturulur ve 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) PSHE, SRE, Citizenshipand Computing / BİT programlarına dahil edilecek ve hem güvenli okul hem de evde kullanımını kapsayacaktır.
* Kabul Edilebilir Kullanım beklentileri 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 katılımı ve eğitimi

* Çevrimiçi güvenlik (e-Güvenlik) politikası, tüm çalışanların katılımı için resmi olarak sağlanacak ve tartışılacak ve korunma sorumluluğumuzun bir parçası olarak güçlendirilecek ve vurgulanacaktır.
* Personel, İnternet trafiğinin izlenebileceğini ve tek bir kullanıcıya kadar izlenebileceğinin farkında olacak. 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.

Ebeveynlerin katılımı ve eğitimi

* Aşağıbağlar Anaokulu, 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.
* Okullarımızın bir parçası olarak ebeveynlerin çevrimiçi güvenlik bilgilerini okumaları istenecektir.
* Ebeveynler, Okula Kabul Edilebilir Kullanım Politikası´nı okumaya ve çocuklarıyla etkilerini tartışmaya teşvik edilecektir.
* Çevrimiçi güvenlik konusundaki ebeveynler için bilgi ve rehberlik, ebeveynlere çeşitli biçimlerde sunulacaktır.
* Ebeveynlerin, çevrimiçi olarak çocukları için olumlu davranışları rol modellemeleri teşvik edilecektir.

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