İSTAŞ KENTAŞ ORTAOKULU eGüvenlik Okul Politikası

1. Çevrimiçi Güvenlik Etik Kuralları Oluşturma

1. Amaçlar ve politika kapsamı
2. Olası beyanlar:

- İstaş Kentaş Ortaokulu, çevrimiçi güvenlik (eGüvenlik), bilgisayarlar, tabletler, cep telefonları veya oyun konsolları gibi teknolojiyi kullanırken, dijital dünyadaki çocukların ve yetişkinlerin korunması için vazgeçilmez bir unsur olduğuna inanmaktadır.
- İstaş Kentaş Ortaokulu, 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.
- İstaş Kentaş Ortaokulu, eğitim standartlarını yükseltmek, başarıyı teşvik etmek, personelin mesleki çalışmalarını desteklemek ve yönetim işlevlerini geliştirmek için toplumun kaliteli İnternet erişimi sunma yükümlülüğüne sahiptir.
- İstaş Kentaş Ortaokulu, tüm çocukların ve personelin çevrimiçi olarak potansiyel zararlardan korunmasını sağlamak için açık bir görev bulunduğunu belirtir.
- İstaş Kentaş Ortaokulu çevrimiçi güvenlik politikasının amacı şudur:
- İstaş Kentaş Ortaokulu güvenli ve güvenli bir ortam olduğundan emin olmak için, toplumun tüm üyelerinden beklenen kilit ilkeleri, güvenli ve sorumlu kullanım teknolojisi ile ilgili olarak tanımlayın.
- İstaş Kentaş Ortaokulu topluluğunun tüm üyelerini çevrimiçi olarak koruyun ve koruyun.
- Bilimin potansiyel riskleri ve yararları konusunda Silifke Cumhuriyet İlkokulu topluluğunun tüm üyeleri ile farkındalık yaratın.
- Tüm personelin güvenli ve sorumlu bir şekilde çalışmasını sağlamak, olumlu davranışları online olarak modellemek ve teknolojiyi kullanırken kendi standartlarını ve uygulamalarını yönetme gereksiniminin farkında olun.
- Topluluğun tüm üyeleri tarafından bilinen çevrimiçi güvenlik endişelerine yanıt verirken açıkça kullanılacak prosedürleri tanımlayın.
- 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) dahil olmak üzere tüm personel için geçerlidir) yanı sıra çocuklar ve ebeveynler / bakıcılar.
- Bu politika, internet erişimi ve kişisel cihazlar da dahil 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 verilir telefonları.
- Bu politika, koruma ve çocuk koruma, zorbalığa maruz kalma, davranış, veri güvenliği, görüntü kullanımı, Kabul Edilebilir Kullanım Politikaları, gizlilik, tarama, arama ve müsadere ve ilgili müfredat dahil olmak üzere diğer ilgili okul politikaları ile birlikte okunmalıdır. Bilişim / BİT, Kişisel Sosyal ve Sağlık Eğitimi (PSHE), Vatandaşlık ve Cinsellik ve İlişkiler Eğitimi (SRE) gibi politikalar.

1.2 Çevrimiçi güvenlik politikası yazma ve gözden geçirme

1. Olası beyanlar:

Belirlenmiş Koruyucu Kurşun (DSL) .....

Yönetim Organının Çevrimiçi güvenlik (eGüvenliği) .....

Okul müdürü tarafından onaylanan politika: ..... Tarih: .....

Yönetim Organının Politika : ..... Tarih: .....

Bir sonraki politika gözden geçirme tarihi: .....

- İstaş Kentaş Ortaokulu Online güvenlik politikası, personel, öğrenciler ve ebeveynleri / bakıcıları içeren, gerektiğinde uzman tavsiyesi ve girişi ile okul tarafından yazılmıştır.
- Politika, liderlik / yönetim ekibi ve Yönetim Kuruluşu tarafından onaylandı ve kabul edildi.
- Okul, online güvenlik (eGüvenlik) için baş sorumluluğu üstlenmek üzere Hakim Vücudunun üyesi olarak Müdür Yardımcısını atandı.
- Çevrimiçi güvenlik (eGüvenlik) 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. 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 meselesidir ve güçlü bir çevrimiçi güvenlik kültürü proaktif olarak incelenmesini sağlayın.
- Onların çevrimiçi güvenlik rolü ve sorumluluklarını yerine getirmek için yeterli zaman ve kaynağa sahip olmalarını sağlayarak Belirlenmiş Koruyucu Kurşunun (DSL) desteklenmesi.
- Çevrimiçi güvenlikle ilgili uygun ve güncel politikaların ve prosedürlerin bulunmasını sağlayın, uygun profesyonel davranışı ve teknolojinin kullanımını kapsayan Kabul Edilebilir Kullanım Politikası da dahil olmak üzere.
- 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 / ayar sistemlerinin ve ağlarının güvenliğini ve güvenliğini izlemek ve okul / ayar 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.
- Okul, yerel ve ulusal destek dahil olmak üzere çevrimiçi güvenlik endişeleri ile ilgili olarak erişmek için okul / çevre topluluğu için sağlam raporlama kanallarının bulunmasını sağlayın.
- Cihazların güvenli ve sorumlu kullanılmasını sağlamak da dahil olmak üzere, teknolojinin güvenli kullanımı ile ilgili uygun risk değerlendirmelerinin yapılmasını sağlayın.
- Yönetim Organının üyesi olan çevrimiçi güvenliğin sağlanmasına ilişkin bir sorumluluk üstlenmesinin sağlanması.
- İyileştirme güç ve alanlarını belirlemek için mevcut çevrimiçi güvenlik uygulamasını denetlemek ve değerlendirmek.
- Belirlenmiş Koruyucu Kurşun (DSL), çevrimiçi güvenlik sorumlusu ile birlikte çalışmasını sağlamak için. (Aynı kişi değillerse, bkz. Bölüm 1.3.2)

1.3.2 Belirlenmiş Koruyucu Kurşunun 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, bakıcılara ve daha geniş topluluğa terfi edilmesini sağlama.
- Uygulamanın mevcut mevzuata uygun olmasını sağlamak için veri koruma ve veri güvenliği için okul / kurucu kurmayla birlikte çalışın.
- Çevrimiçi güvenlik endişelerinin / olaylarının ve kayıt yapılarını ve mekanizmalarını koruyan okulların bir parçası olarak alınan önlemlerin kayıtlarının tutulması.

Boşlukları / eğilimleri belirlemek için okul / ayarlardaki çevrimiçi güvenlik olaylarını izleyin ve gereksinimi yansıtacak şekilde okul / ayarlar eğitim cevabını güncellemek için bu verileri kullanın.

- Okul yönetim ekibine, Yönetim Organına ve diğer acentelere, çevrimiçi güvenlik endişeleri ve yerel veriler / rakamlar hakkında rapor vermek.
- Yerel ve ulusal kurumlarla irtibat kurun.
- Paydaş girişi 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 (en az yılda bir kez).
- Çevrimiçi güvenliğin diğer uygun okul politikaları ve prosedürleriyle bütünleştirilmesini sağlama.

1.3.3 Tüm çalışanların kilit sorumlulukları şunlardır:

- Çevrimiçi güvenlik politikalarının geliştirilmesine katkıda bulunmak.
- Okulu Okumak Kabul Edilebilir Kullanım Politikaları (AUP´lar) ve onlara bağlı kalarak.
- Okul / tesisat sistemlerinin ve verilerin güvenliğinden sorumlu tutulmak.
- 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 olan yerlerde müfredat teslimatı için çevrimiçi güvenlik eğitimi gömülmesi.
- 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 konularda, dahili 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 yapılması.
- Bu alanda mesleki gelişim için kişisel sorumluluk alıyor.

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 / ortamın ağının düzenli olarak izlenmesini sağlamak ve kasıtlı ya da yanlışlıkla yapılan yanlış kullanımı DSL´ye bildirmek.
- Herhangi bir ihlal veya endişeyi DSL ve liderlik ekibine rapor edin ve birlikte kaydedilmesini ve uygun önlemlerin tavsiye edildiği şekilde alınmasını sağlayın.
- 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 kurun.
- Özellikle uygun çevrimiçi güvenlik politikaları ve prosedürlerinin geliştirilmesi ve uygulanmasında DSL ve liderlik ekibine teknik destek ve perspektif sağlamak.
- Okulun BİT altyapısının / sisteminin güvenli olduğunu ve kötüye kullanım veya kötü niyetli saldırılara açık olmamasını sağlamak.
- Tüm ayarlama makinelerinde ve taşınabilir aygıtlarda uygun anti-virüs yazılımının ve sistem güncellemelerinin kurulup kurulmadığından emin olun.
- Uygun olan güçlü parolaların en genç kullanıcıları hariç olmak üzere tümüne uygulandığından ve uygulandığından emin olun.

1.3.5 Çocukların ve gençlerin başlıca sorumlulukları şunlardır:

- Çevrimiçi güvenlik politikalarının geliştirilmesine katkıda bulunmak.
- Okul okumak / Kabul Edilebilir Kullanım Politikaları (AUP´lar) koymak 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.

Bireysel yaşlarına, yeteneklerine ve zayıf yönlerine uygun bir seviyede:

- Kendilerini ve başkalarını çevrimiçi olarak korumak için sorumluluk alıyor.
- 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 ve bakıcıların başlıca sorumlulukları şunlardır:

- Okul okumak / Kabul Edilebilir Kullanım Politikalarını belirlemek, çocuklarını kendilerine bağlı kalmaya teşvik etmek ve uygun olduğunda kendilerine bağlı kalmak.
- Çocuklarıyla çevrimiçi güvenlik konularını tartışmak, okulun çevrimiçi güvenlik yaklaşımlarını desteklemek ve evde uygun güvenli çevrimiçi davranışları pekiştirmek.
- Teknoloji ve sosyal medyanın güvenli ve uygun kullanım modellemesi.
- Davranışlarında, çocuğun çevrimiçi olarak zarar görme tehlikesi altında olduğunu gösteren değişiklikleri belirleme.
- Okul veya diğer uygun kurumlardan, çevrimiçi problem veya endişelerle karşılaşırsa yardım veya destek isteyin.
- Okulun / çevrimiçi güvenlik politikalarının oluşturulmasına katkıda bulunmak.
- Öğrenme platformları ve diğer ağ kaynakları gibi okul sistemlerini güvenli ve uygun bir şekilde kullanma.
- Yeni ve gelişmekte olan teknolojilerin getirdiği 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 sitesindeki iletişim bilgileri okul / ayar adresi, e-posta ve telefon numarası olacaktır. Personel veya öğrencilerin kişisel bilgileri yayınlanmayacak.
- Kafa öğretmeni / yöneticisi 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 için hasat görmemek için (örn. ´@´ Yerine ´AT´ yazısı girilerek) e-posta adresleri çevrimiçi olarak dikkatli bir şekilde yayınlanacaktır.
- Öğrenci çalışmaları izniyle ya da ebeveynlerinin / bakıcılarının izniyle yayınlanacaktır.
- Okul web sitesinin yönetici hesabı, uygun bir şekilde şifrelenerek korunacaktır.
- Okul, çevrimiçi güvenlik dahil olmak üzere, toplumun üyeleri için okul web sitesinde korunma hakkında bilgi gönderecektir.

2.2 Çevrimiçi görüntü ve videolar yayınlama

Olası beyanlar:

- Okul / ortam, çevrimiçi paylaşılan tüm resimlerin ve videoların okul resim kullanımı politikasına uygun şekilde kullanılmasını sağlayacaktır.
- Okul / ortam, 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 ebeveynlerin veya bakıcıların yazılı izni her zaman elde edilecektir.

2.3 E-postaları yönetme

Tüm ayarlar için önemlidir

2.3 Olası beyanlar:

- Öğrenciler eğitim amacıyla yalnızca okul / ayarlı e-posta hesapları kullanabilir
- Personelin tüm üyelerine resmi bir iletişim için kullanılacak belirli bir okul / ayar e-posta adresi verilir.
- Personel tarafından herhangi bir resmi okul / işyerinde kişisel e-posta adresinin kullanılması yasaktır.
- Zincir mesajlarının / e-postalarının vb. iletilmesine izin verilmez. Spam veya önemsiz posta engellenecek ve e-posta sağlayıcısına bildirilecektir.
- Veri koruma mevzuatına tabi olabilecek herhangi bir içeriği (örn. Hassas veya kişisel bilgiler) içeren herhangi bir elektronik iletişim yalnızca güvenli ve şifrelenmiş bir e-posta ile gönderilecektir.
- Okul / ayarı e-posta sistemlerine erişim her zaman veri koruma yasalarına uygun olarak ve diğer uygun okul / ayar politikalarına (örn. Gizlilik) uygun olarak gerçekleşecektir.
- Topluluk üyeleri, saldırgan bir iletişim kurdukları takdirde derhal belirlenmiş bir personele haber vermekle yükümlüdürler ve bu dosyalar okulun dosyalarından / kayıtlarından korunacaktır.
- Okulun dışındaki iletişim için tüm sınıf veya grup e-posta adresleri kullanılabilir.
- Personel, e-postaya yanıt verirken, özellikle personel, öğrenciler ve ebeveynler arasında iletişim kurulması halinde, uygun bir iş hayatı dengesi geliştirmeye teşvik edilecektir.
- Aşırı sosyal e-posta kullanımı öğretme ve öğrenmeyi etkileyebilir ve kısıtlanabilir. Okuldaki harici kişisel e-posta hesaplarına erişim engellenmiş olabilir.

- Dış organizasyonlara gönderilen e-postalar gönderilmeden önce dikkatli ve yetkili olarak yazılmalı, okuldaki kağıda yazılmış bir mektup da aynı şekilde olacaktır.
- Okul, refah ve pastoral meseleleri bildiren özel bir e-postaya sahip olacak. Bu gelen kutusu, belirlenmiş ve eğitilmiş personel tarafından yönetilecektir.
- Okulun e-posta adresleri ve diğer resmi iletişim bilgileri, kişisel sosyal medya hesapları oluşturmak için kullanılamaz.

2.4 Eğitim amaçlı resmi video konferans ve web kamerası kullanımı

2.4 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, otomatik cevaplamaya ayarlanmadığında kapatılacaktır.
- Harici IP adresleri diğer sitelere sunulmayacaktır.
- Video konferans iletişim detayları kamuoyuna açıklanmamıştır.
- Video konferans ekipmanları güvenli bir şekilde tutulacak ve gerekirse kullanılmadığında kilitlenecektir.
- Okul video konferans ekipmanları izinsiz olarak okul binalarından alınmayacaktır.
- 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 güvenli 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.
- Veliler ve bakıcıların rızası, çocuklar video konferans faaliyetlerine katılmadan önce edinilecektir.
- 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 verilmektedir.
- Eğitimli video konferans servisleri için benzersiz oturum açma ve şifre bilgileri yalnızca personel üyelerine verilecek ve güvence altına alınmış olacak.

içerik

- 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.

2.5 İnternetin ve ilgili cihazların uygun ve güvenli derslik kullanımı

2.5 Olası beyanlar:

- İnternet kullanımı eğitim erişiminin önemli bir özelliğidir ve tüm çocuklar gömülü bir bütün okul müfredatının bir parçası olarak endişeleri 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 dayanamayacaklarının farkındadır ve gözetim, sınıf yönetimi ve güvenli ve sorumlu kullanım eğitimi önemlidir.
- Öğrencilerin Denetleme 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 dahil 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 materyalleri eleştirel olarak öğrenecekleri ve bilgilerin doğruluğunu kabul etmeden nasıl doğrulanacağı gösterilecektir.
    - Çevrimiçi materyallerin değerlendirilmesi, her konuda öğretme ve öğrenmenin bir parçasıdır ve müfredatta bir bütün okul / zorunluluk şartı olarak görülür.
    - Okul, öğrencileri ve çalışanlarımızın güvenli ve güvenli bir ortamda iletişim kurmalarını ve işbirliği yapmalarını sağlamak için interneti kullanacaklardır.

3. Kişisel Cihazların ve Cep Telefonlarının Kullanımı

Tartışma:

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 İstaş Kentaş Ortaokulu 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 / tesis tarafından kararlaştırılacak ve okul Kabul Edilebilir Kullanım veya Cep Telefonu Politikası dahil olmak üzere uygun politikalarda yer alacaktır.
- İstaş Kentaş Ortaokulu, mobil teknolojilerle yapılan kişisel iletişimin, çocuklar, personel ve anne-baba / bakıcılar için gündelik yaşamın kabul edilen bir parçası olduğunun farkındadır; ancak, bu tür teknolojilerin okul / ortamlarda 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 tümü yasaya ve diğer uygun okul politikalarına uygun olarak yerinde olacaktır .
- Sahada getirilen her türlü elektronik cihazın sorumluluğu kullanıcıya aittir. Okulun / ortamın, bu tür öğelerin kaybı, çalınması veya zarar görmesi konusunda sorumluluk kabul etmemesi. Okul / ortam, 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 yasaklanmış ve herhangi bir ihlal, disiplin / davranış politikasının bir parçası olarak ele alınacaktır.
- İstaş Kentaş Ortaokulu topluluğunun tüm üyelerine cep telefonlarını veya cihazlarını kayıp, hırsızlık veya hasardan korumak için adım atmaları önerilir.
- İstaş Kentaş Ortaokulu 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.
- İstaş Kentaş Ortaokulu 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 Öğrenciler kişisel cihazların ve cep telefonlarının 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.
- Personel üyelerinin, çocukların cep telefonlarını veya kişisel cihazlarını bir eğitim etkinliği kapsamında kullanmalarına izin vermek için eğitimsel bir nedeni varsa, bu yalnızca Liderlik Ekibi tarafından onaylandığında gerçekleşecektir.
- Bir öğrencinin ebeveynlerine / bakıcılarına başvurması gerekiyorsa, bir okul / ayar telefonu kullanmasına izin verilecektir.
- Ebeveynlerin okul gününde cep telefonuyla çocuklarıyla iletişim kurmamaları, okul ofisine başvurmaları önerilir. İstisnai durumlarda istisnai durumlara istinaden ve öğretmenin onayladığı şekilde istisnalara izin verilebilir.
- Öğrenciler, yalnızca güvenilir arkadaşlarına ve aile üyelerine vererek telefon numaralarını korumalıdır.
- Öğrencilere, cep telefonlarının ve kişisel cihazların güvenli ve uygun bir şekilde kullanılmaları öğretilecek ve sınırların ve sonuçların farkına varılacaktır.
- Okul personeli, okul davranışını veya zorbalık politikasını ihlal etmek için kullanıldığına veya gençlerin ürettiği cinsel imgelemi (cinsel tercihler) içerebileceğine inanıyorsa, bir öğrencinin cep telefonuna veya cihazına el koyabilir. Telefon veya cihaz, öğrencinin veya veli / bakıcının onayı ile Liderlik ekibinin bir üyesi tarafından aranabilir ve uygunsa, içerik silinebilir veya silinmek üzere talep edilebilir. Cep telefonu veya kişisel cihazların aranması yalnızca okul politikasına uygun olarak yapılacaktır.
- 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 konudan ödün verebilecek önceden var olan ilişkiler, liderler / yöneticilerle tartışılacaktır.
- 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 iş tarafından sağlanan ekipmanı kullanır.
- Personel üyeleri, kişisel telefonların ve cihazların herhangi bir şekilde kullanımının daima veri koruma ve ilgili okul politikası ve prosedürleri (örn. Gizlilik, veri güvenliği, Kabul Edilebilir Kullanım vb .) Gibi yasa 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 liderlik ekibinin bir üyesi 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 personelin okul / ilke 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 iddiaa okul / ayar iddiaları yönetim politikasını izleyerek yanıt verilecektir.

3.5 Ziyaretçiler kişisel cihazların ve cep telefonlarının kullanılması

3.5 Olası Bildirimler:

- Ebeveynler / bakıcılar ve ziyaretçiler, okul / ayarlar kabul edilebilir kullanım politikasına uygun olarak cep telefonlarını ve kişisel cihazları kullanmalıdır.
- Fotoğraflar veya videolar çekmek için ziyaretçiler, ebeveynler / bakıcılar 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, endişeleri güvende ve uygun olduğunda itiraf etmesi beklenir ve her zaman ziyaretçilerin herhangi bir ihlalini Belirlenmiş Korunma Kur´una bildireceklerdir.

4. Politika Kararları

4.1. Çevrimiçi riskleri azaltmak

4.1 Olası beyanlar:

- Silifke Cumhuriyet İlkokulu 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 kullanılmadan önce uygun risk değerlendirmelerinin yapılmasına izin verecektir.
- 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 (eGüvenlik) 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 (eGüvenlik) 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 girdileri 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 (eGüvenlik) PSHE, SRE, Citizenship and Computing / BİT programlarına dahil edilecek ve hem güvenli okul hem de evde kullanımını kapsayacaktır.
- Kabul Edilebilir Kullanım beklentileri ve Postalar, Internet erişimi olan tüm odalarda yayınlanacaktır.
- İnternetin ve teknolojinin güvenli ve sorumlu kullanımı, müfredatta ve tüm konularda güçlenecektir.
- Dışarıdan destek, okulların dahili çevrimiçi güvenlik (eGüvenlik) eğitim yaklaşımlarını tamamlamak ve desteklemek için kullanılacaktır.
- Okul, öğrencilerin teknolojiyi olumlu şekilde kullandıklarını ödüllendirecek.
- Okul, öğrencilerin ihtiyaçlarına uygun olarak çevrimiçi güvenliği geliştirmek için akran eğitimini uygulayacaktır.

5.2 Savunmasız kabul edilen çocukların ve gençlerin katılımı ve eğitimi

5.2 Olası ifade:

- İstaş Kentaş Ortaokulu, bir takım faktörlerden dolayı bazı çocukların çevrimiçi ortamda daha savunmasız olduğu düşünülmektedir.

5.3 Personelin katılımı ve eğitimi

5.3 Olası beyanlar:

- Çevrimiçi güvenlik (eGüvenlik) 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 çevrimiçi davranışlarının okuldaki rolü ve itibarını etkileyebileceğinin farkına varacaktır. Mesleği veya kurumu çürüme durumuna düşürdüğü veya profesyonel yeteneklerine güvenini kaybetmiş bir şeyin bulunduğu düşünülürse, hukuk, 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 / ortam, çalışanların öğrencilerin yaşlarına ve yeteneklerine göre kullanması gereken yararlı çevrimiçi araçları vurgulamaktadır.

5.4 Anababalar ve bakıcıların katılımı ve eğitimi

5.4 Olası beyanlar:

- İstaş Kentaş Ortaokulu, çocukların internetin ve dijital teknolojinin güvenilir ve sorumlu kullanıcıları olabilmesi için ana-babanın / bakıcıların oynayacakları önemli bir role sahip olduklarını kabul eder.
- Ebeveynlerin dikkatleri, bültenler, mektuplar, okul izahname ve okul web sitesinde okul çevrimiçi güvenlik (eGüvenlik) politikasına ve beklentilerine yönelecektir.
- Evde ve okulda ebeveynlerle çevrimiçi güvenlik konusundaki ortaklık yaklaşımı teşvik edilecektir. Bu, güvenli ana sayfa İnternet kullanımı için gösteriler ve öneriler içeren ebeveyn akşamları sunma veya ebeveyn akşamları, geçiş olayları, bayramlar ve spor günleri gibi diğer iyi katılan etkinliklerde çevrimiçi güvenliğin vurgulanmasını içerebilir.
- Ana Okul Anlaşması´nın 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.
- Ebeveynler, çevrimiçi olarak çocukları için rol modeli olumlu davranışlar teşvik edilecektir.

6. Çevrimiçi Olaylara Yanıt Verme ve Endişeleri Koruma

Olası beyanlar:

- Topluluğun tüm üyeleri, cinsel tercih, çevrimiçi / siber zorbalık vb. dahil olmak üzere karşılaşılabilecek çevrimiçi risklerin çeşitliliğinden haberdar edilecektir. Bu, öğrencilere yönelik personel eğitimi ve eğitim yaklaşımları içerisinde vurgulanacaktır.
- Okul / çevre topluluğunun tüm üyeleri, filtreleme, cinsel tercih etme, siber zorbalık, yasadışı içerik ihlali vb. Gibi çevrimiçi güvenlik (eGüvenlik) endişelerini bildirme prosedürü hakkında bilgilendirilecektir.
- Belirlenmiş Koruyucu Kurşun (DSL), daha sonra kaydedilecek olan çocuk koruma endişelerini içeren herhangi bir çevrimiçi güvenlik (eGüvenlik) 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 baş öğretmenine yönlendirilecektir
- Okul şikayet prosedürü öğrencilere, velilere ve personele bildirilecektir.
- Şikayet ve ihbar prosedürü personele bildirilecektir.
- Okul topluluğunun tüm üyeleri, gizliliğin öneminden ve endişeleri bildirmek için resmi okul usullerine uyma ihtiyacından haberdar olmalıdırlar.
- Okul topluluğunun 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 (eGüvenlik) olaylarını, uygun olduğunda, okul disiplini / davranış politikasına uygun olarak yönetir.
- Okul, ebeveynleri / bakıcıları, ihtiyaç duyulduğunda ve bunlarla ilgili endişeleri bildirir.
- Herhangi bir soruşturma tamamlandıktan sonra okul okunacak, öğrenilen dersleri belirleyecek ve değişiklikleri gerektiği gibi uygulayacaktır.
- Sorunları çözmek için ebeveynlerin ve çocukların okulla ortak çalışması gerek.

1. Creating an Online Safety Ethos

1.1 Aims and policy scope

1.1. Possible statements:

* İstaş Kentaş Ortaokulu believes that online safety (e-Safety) is an essential element of safeguarding children and adults in the digital world, when using technology such as computers, tablets, mobile phones or games consoles.

* İstaş Kentaş Ortaokulu identifies that the internet and information communication technologies are an important part of everyday life, so children must be supported to be able to learn how to develop strategies to manage and respond to risk and be empowered to build resilience online.

* İstaş Kentaş Ortaokulu has a duty to provide the community with quality Internet access to raise education standards, promote achievement, support professional work of staff and enhance management functions.

* İstaş Kentaş Ortaokulu identifies that there is a clear duty to ensure that all children and staff are protected from potential harm online.

* The purpose of İstaş Kentaş Ortaokulu online safety policy is to:

- Clearly identify the key principles expected of all members of the community with regards to the safe and responsible use technology to ensure that İstaş Kentaş Ortaokulu is a safe and secure environment.
- Safeguard and protect all members of İstaş Kentaş Ortaokulu community online.
- Raise awareness with all members of İstaş Kentaş Ortaokulu community regarding the potential risks as well as benefits of technology.
- To enable all staff to work safely and responsibly, to role model positive behaviour online and be aware of the need to manage their own standards and practice when using technology.
- Identify clear procedures to use when responding to online safety concerns that are known by all members of the community.

* This policy applies to all staff including the, teachers, support staff, external contractors , visitors, volunteers and other individuals who work for or provide services on behalf of the school (collectively referred to as 'staff' in this policy) as well as children and parents/carers.

* This policy applies to all access to the internet and use of information communication devices, including personal devices, or where children, staff or other individuals have been provided with school issued devices for use off-site, such as a work laptops, tablets or mobile phones.

* This policy must be read in conjunction with other relevant school policies including safeguarding and child protection, anti-bullying, behaviour, data security, image use, Acceptable Use Policies, confidentiality, screening, searching and confiscation and relevant curriculum policies including computing/ICT, Personal Social and Health Education (PSHE), Citizenship and Sex and Relationships Education (SRE).

1.2 Writing and reviewing the online safety policy

1.2 Possible statements:

The Designated Safeguarding Lead (DSL) is.....

The Online safety (e-Safety) lead for the is.....

Policy approved by Head Teacher/Manager: ..... Date: .....

Policy approved by: ..... Date: .....

The date for the next policy review is: .....

* İstaş Kentaş Ortaokulu online safety policy has been written by the school, involving staff, pupils and parents/carers, with specialist advice and input as required.

* The policy has been approved and agreed by the Leadership/Management Team and Governing Body.

* The school has appointed assistant director as the member of the Governing Body to take lead responsibility for online safety (e-Safety).

* The online safety (e–Safety) Policy and its implementation will be reviewed by the school/setting at least annually or sooner if required.

1.3 Key responsibilities forthe community

1.3.1 The key responsibilities of the school/setting management and leadership team are:

* Developing, owning and promoting the online safety vision and culture to all stakeholders, in line with national and local recommendations with appropriate support and consultation throughout the school community.

* Ensuring that online safety is viewed by the whole community as a safeguarding issue and proactively developing a robust online safety culture.

* Supporting the Designated Safeguarding Lead (DSL) by ensuring they have sufficient time and resources to fulfil their online safety role and responsibilities.

* Ensuring there are appropriate and up-to-date policies and procedures regarding online safety including an Acceptable Use Policy which covers appropriate professional conduct and use of technology.

* To ensure that suitable and appropriate filtering and monitoring systems are in place to protect children from inappropriate content which meet the needs of the school community whilst ensuring children have access to required educational material.

* To work with and support technical staff in monitoring the safety and security of school/setting systems and networks and to ensure that the school/setting network system is actively monitored.

* Ensuring all members of staff receive regular, up-to-date and appropriate training regarding online safety roles and responsibilities and provide guidance regarding safe appropriate communications.

* Ensuring that online safety is embedded within a progressive whole school/setting curriculum which enables all pupils to develop an age-appropriate understanding of online safety and the associated risks and safe behaviours.

* To be aware ofany online safety incidents and ensure that external agencies and supportare liaised with as appropriate.

* Receiving and regularly reviewing online safeguarding records and using them to inform and shape future practice.

* Ensuring there are robust reporting channels for the school/setting community to access regarding online safety concerns, including internal, local and national support.

* Ensure that appropriate risk assessments are undertaken regarding the safe use of technology, including ensuring the safe and responsible use of devices.

* To ensure a member of the Governing Body is identified with a lead responsibility for supporting online safety.

- Auditing and evaluating current online safety practice to identify strengths and areas for improvement.
- To ensure that the Designated Safeguarding Lead (DSL) works with the online safety lead.
-

1.3.2 The key responsibilities of the Designated Safeguarding Lead are:

* Acting as a named point of contact on all online safeguarding issues and liaising with other members of staff and other agencies as appropriate.

* Keeping up-to-date with current research, legislation and trends regarding online safety.

* Coordinating participation in local and national events to promote positive online behaviour, e.g. Safer Internet Day.

* Ensuring that online safety is promoted to parents and carers and the wider community through a variety of channels and approaches.

* Work with the school/setting lead for data protection and data security to ensure that practice is in line with current legislation.

* Maintaining a record of online safety concerns/incidents and actions taken as part of the schools safeguarding recording structures and mechanisms.

* Monitor the school/settings online safety incidents to identify gaps/trends and use this data to update the school/settings education response to reflect need.

* To report to the school management team, Governing Body and other agencies as appropriate, on online safety concerns and local data/figures.

* Liaising with local and national bodies, as appropriate.

* Working with the school/setting leadership and management to review and update the online safety policies, Acceptable Use Policies (AUPs) and other related policies on a regular basis (at least annually) with stakeholder input.

* Ensuring that online safety is integrated with other appropriate school policies and procedures.

1.3.3 The key responsibilities for all members of staff are:

* Contributing to the development of online safety policies.

* Reading the school Acceptable Use Policies (AUPs) and adhering to them.

* Taking responsibility for the security of school/setting systems and data.

* Having an awareness of a range of different online safety issues and how they may relate to the children in their care.

* Modelling good practice when using new and emerging technologies

* Embedding online safety education in curriculum delivery wherever possible.

* Identifying individuals of concern and taking appropriate action by following school safeguarding policies and procedures.

* Knowing when and how to escalate online safety issues, internally and externally.

* Being able to signpost to appropriate support available for online safety issues, internally and externally.

* Maintaining a professional level of conduct in their personal use of technology, both on and off site.

- Demonstrating an emphasis on positive learning opportunities.
- Taking personal responsibility for professional development in this area.

1.3.4 In addition to the above, the key responsibilities for staff managing the technical environment are:

* Providing a safe and secure technical infrastructure which support safe online practices while ensuring that learning opportunities are still maximised.

* Taking responsibility for the implementation of safe security of systems and data in partnership with the leadership and management team.

* To ensure that suitable access controls and encryption is implemented to protect personal and sensitive information held on school-owned devices.

* Ensuring that the schools filtering policy is applied and updated on a regular basis and that responsibility for its implementation is shared with the DSL.

* Ensuring that the use of the school/setting's network is regularly monitored and reporting any deliberate or accidental misuse to the DSL.

* Report any breaches or concerns to the DSLand leadership team and together ensure that they are recorded and appropriate action is taken as advised.

* Developing an understanding of the relevant legislation as it relates to the security and safety of the technical infrastructure.

* Report any breaches and liaising with the local authority (or other local or national bodies) as appropriate on technical infrastructure issues.

* Providing technical support and perspective to the DSL and leadership team, especially in the development and implementation of appropriate online safety policies and procedures.

- Ensuring that the school's ICT infrastructure/system is secure and not open to misuse or malicious attack.
- Ensuring that appropriate anti-virus software and system updates are installed and maintained on all setting machines and portable devices.
- Ensure that appropriately strong passwords are applied and enforced for all but the youngest users.

1.3.5 The key responsibilities of children and young people are:

* Contributing to the development of online safety policies.

* Reading the school/setting Acceptable Use Policies (AUPs) and adhering to them.

* Respecting the feelings and rights of others both on and offline.

* Seeking help from a trusted adult if things go wrong, and supporting others that may be experiencing online safety issues.

At a level that is appropriate to their individual age, ability and vulnerabilities:

* Taking responsibility for keeping themselves and others safe online.

* Taking responsibility for their own awareness and learning in relation to the opportunities and risks posed by new and emerging technologies.

* Assessing the personal risks of using any particular technology, and behaving safely and responsibly to limit those risks.

1.3.6 The key responsibilities of parents and carers are:

* Reading the school/setting Acceptable Use Policies, encouraging their children to adhere to them, and adhering to them themselves where appropriate.

* Discussing online safety issues with their children, supporting the school in their online safety approaches, and reinfo