

ALTINOVA ATATÜRK İLKOKULU E-GÜVENLİK POLİTİKASI

EGÜVENLİK KABUL EDİLEBİLİR KULLANIM POLİTİKASI

BİLGİLENDİRME METNİ

1. AMAÇ

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

2. E-GÜVENLİK (E-SAFETY) POLİTİKAMIZ:

- Okulumuzda ders anlatımı yapılan her alanda etkileşimli tahta ve güvenli internet erişim ağı vardır. Ders anlatımlarında eba eğitim ve eTwinning portallarından da yararlanılmaktadır. Güvenli internet erişim ağı, ağ güvenlik filtresiyle kullanılmaktadır.
- Okulumuzun internet sitesi, facebook gibi sosyal ağları bulunmaktadır. Bu ağların üzerinde yayımlanan veriler kontrollü olarak paylaşılmaktadır.
- Etkileşimli tahtalar güvenlik kurulumu ile öğretmenlerin kontrolünde kullanılmaktadır.
- Okul projelerimiz kapsamında internetin doğru ve güvenli kullanımı, Siber Zorbalık gibi konularda seminerler tertiplenmektedir.
- Okulumuzda etkileşimli tahtalar, güvenli erişim ağı ve eba eğitim ve eTwinning portallarının kullanımının yoğun olması nedeniyle zümre öğretmenleri tarafından her zümrede BİT'nin doğru ve güvenli kullanımı, yapılan alıntıların derslere ve ödevlere aktarımı(kaynak kullanımı) ile ilgili kararlar alınmakta ve öğrenciler bu yönde bilgilendirilmektedir.
- Okulumuzun öğretmenleri Milli Eğitim Bakanlığı tarafından verilen Siber Zorbalık, BİT'in doğru ve güvenli kullanımı konularında uzaktan ve yüz yüze eğitimler almıştır/alacaktır.
- Okulumuzda her yıl "Daha Güvenli İnternet Günü" kutlaması amaçlanmaktadır.
- Okul paydaşlarımız istedikleri zaman konu ile ilgili bilgi alabilmekteler.
- Okulumuzda 21.yy iletişim becerileri önemsenmektedir. Bununla ilgili olarak öğrencilerimizin BİT kullanım becerilerini geliştirme çalışmaları yapılmaktadır.
- Okulumuzda Dijital vatandaş olma konusunda paydaşlarımızı bilinçlendirme çalışmaları yapılmaktadır.
- Okulumuzda izinsiz fotoğraf çekmek kesinlikle yasaktır.

- Okulumuzun öğrencilerinin yüzleri okula ait hiçbir sosyal medya sitesinde ve eTwinningportali dahilindeki proje resimlerinde açık bir şekilde gösterilmeyecektir.
- Öğrencilerimizin ve velilerimizin okulumuza kayıt olurken sağladıkları kişisel bilgileri idare sorumluluğunda ve tarafından korunmaktadır.
- Velilerimizin iletişim bilgileri kendi bilgi ve istekleri haricinde asla 3. Şahıslarla paylaşamaz.

3. SORUMLULUKLAR

Bu politikanın uygulatılmasından idare ve öğretmenler sorumludur.

A. TÜM ÇALIŞANLARIN KİLİT SORUMLULUKLARI ŞUNLARDIR:

- Çevrimiçi güvenlik politikalarının geliştirilmesine katkıda bulunmak.
- 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 modelleme ,
- Mümkün olduğunca müfredat ile çevrimiçi güvenlik eğitimini ilişkilendirme.
- Okul koruma politikalarını ve prosedürlerini takip ederek endişe duyan bireylerin belirlenmesi ve uygun önlem alınması.
- Olumlu öğrenme fırsatlarına vurgu yapmak.
- Bu alanda mesleki gelişim için kişisel sorumluluk almak.

B. ÇOCUKLARIN VE GENÇLERİN BAŞLICA SORUMLULUKLARI ŞUNLARDIR:

- Çevrimiçi güvenlik politikalarının geliştirilmesine katkıda bulunmak.
- Okulun Kabul Edilebilir Kullanım 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.
- Bireysel yaşlarına, yeteneklerine ve zayıf yönlerine uygun bir seviyede:
- 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.

C. EBEVEYNLERİN BAŞLICA SORUMLULUKLARI ŞUNLARDIR:

- 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 veya çocukları çevrimiçi problem veya sorunlarla karşılaşırsa yardım veya destek istemek.

- Okulun çevrimiçi güvenlik politikalarının oluşturulmasına katkıda bulunmak.
- Öğrenme platformları ve diğer ağ kaynakları gibi okul sistemlerini güvenli ve uygun bir şekilde kullanmak.
- Yeni ve gelişmekte olan teknolojilerin getirdiği fırsatlar ve risklerle ilgili olarak kendi bilinci ve öğrenimlerinden sorumlu olmak.

4. TANIMLAR

Bilgisayar Sistemleri

Bilgisayar sistemleri her türlü bilgisayar ile ilgili donanım, teçhizat ve fikri mülkiyeti ifade eder. Buna, okulun sahip olduğu, kiraladığı, uyarladığı veya okulun sahipliğinde bulundurduğu, muhafaza altına aldığı veya kontrolü altında olan bilgisayar sistemleri, kişisel bilgisayarlar, mobil cihazlar, bilgisayar ağları ve her türlü yazılım, donanım yazılımı, işletim yazılımı ve uygulama yazılımı dâhildir. Açık olmak adına, “bilgisayar sistemleri” Okul tarafından uyarlanan yerel ağ, bulut veya Internet temelli hizmetleri veya Okul faaliyetlerinin veya Okul verisinin saklanmasında kullanılan genel nitelikli yerel ağ, yürütülmesinde bulut veya Internet temelli hizmetleri kapsar.

5. TEMEL PRENSİPLER

A. OKUL/WEB SİTESİNİN YÖNETİLMESİ

- 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.

B. ÇEVİRİMİÇİ GÖRÜNTÜ VE VİDEOLAR YAYINLAMA

- 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 kullanımını 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.

C. KİŞİSEL CİHAZ VE CEP TELEFONLARININ KULLANIMI

- Cep telefonlarının ve çocukların, gençlerin ve yetişkinler arasındaki diğer kişisel cihazların yaygın bir şekilde sahiplenilmesi, tüm üyelerin cep telefonlarının ve kişisel cihazların sorumlu bir şekilde kullanılmasını sağlamak için gerekli adımları atmalarını gerektirir .

- Çocukların, 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.
- Okulumuz, mobil teknolojilerle yapılan kişisel iletişimin, çocuklar, personel ve anne-babalar için gündelik yaşamın kabul edilen bir parçası olduğunun farkındadır; ancak, bu tür teknolojilerin okulda güvenli ve uygun bir şekilde kullanılmasını gerektirir.

D. ÖĞRENCİLERİN KİŞİSEL CİHAZLARINI VE CEP TELEFONLARINI KULLANIMI

- Öğrenciler, kişisel cihazların ve cep telefonlarının güvenli ve uygun kullanımı konusunda eğitim alacaklardır.
- Bilişim araçlarını, okul yönetimi ile öğretmenin bilgisi ve izni dışında konuşma yaparak, ses ve görüntü alarak, mesaj ve e-mail göndererek, bunları arkadaşlarıyla paylaşarak eğitim-öğretimi olumsuz yönde etkileyecek şekilde kullanmak aynı zamanda okul ders saatleri içerisinde telefon bulundurmamak kesinlikle yasaktır.
- Cep telefonunun amacı dışında kullanımı ihlali olduğunda, öğrenci, telefondaki özel verilerin korunmasını sağlamak amacıyla telefonunu kapatıp ders öğretmenine verir. Ders öğretmeni öğrenci telefonunu ilgili müdür yardımcısına teslim eder. Cep telefonu öğrenci velisine teslim edilinceye kadar güvenli bir yerde tutulur. Velisi dışında telefon kimseye teslim edilmez.
- Çocukların cep telefonlarının ve kişisel cihazların tüm kullanımları, kabul edilebilir kullanım politikasına uygun olarak gerçekleşecektir. Cep telefonları veya kişisel cihazlar, bir öğretmenin 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.
- 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.

E. ZİYARETÇİ KİŞİSEL CİHAZLAR VE CEP TELEFONLARININ KULLANIMI:

- 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.
- İşbu politikaya veya politikanın belli bir duruma uygulanmasına ilişkin her türlü soru okul idaresine iletilir.

▪ E-GÜVENLİK KOMİSYONU

OKUL GÜVENLİK EYLEM PLANI

Z kuşağı olarak tanımlanan teknolojinin içine doğan çocuklarımız ailelerin de rehberliğinden yararlanamamakta hatta ailelerinin kullanmadığı sosyal medya uygulamaları öğrenciler için tercih sebebi olmaktadır. Çocukların ailelerin bu yetersizliklerinden yararlanması, aileleri için ayrı arkadaşlar için ayrı hesaplar kullanması, uygulama ve oyunların simgelerinin (örneğin hesap makinesi) değiştirerek ailelerin atlatılması gibi durumların yaşanmasını olağan hale getirmektedir. Öğrencilerin, teknolojiye olan hakimiyetleri iyi/etkili kullanıyor algısı yaratmakta teknolojinin etkilerinin artarak yaygınlaşmasına sebep olmaktadır. Ailelerin sosyal öğrenmeyle rol model oldukları öğrencilerin olduğu kadar ailelerin de teknolojinin olumsuz etkilerine maruz kaldıkları, öğrencileri ve okul ortamını etkiledikleri ortadadır. Bireyselleşmiş, sosyalliği sadece çevrimiçi ortamlarda karşılayan/asosyal, sanal aylak, doyumsuz, sorumluluklarını aksatan, dikkat süreleri azalmış, duyarsız, bilgiyi sorgulamadan kullanan, bağımlı, hazırcılığa alışmış, gibi özellikler gösteren yetişkin aile bireyleri de teknolojinin olumsuz etkilerini yaşamaktadır. Teknoloji artılarıyla eksileriyle vazgeçilmez hale gelmişken, teknolojinin olumsuz etkilerine ilişkin gelinek nokta öğrencilerin kullanımının kısıtlanması ve yasaklanması mecburiyetini doğurmaktadır. Oysa ki eğiterek ve faydalı etkinliklere yönelterek ilerideki rekabet gücümüzü yükseltmesi ülke olarak dünyanın geldiği noktada var olabilmek için gereklidir. Gençler ve teknoloji, günümüz dünyasında çoğu kez ayrılamaz. Web'in kullanımı artarken, güvenli kullanımıyla da ilgilidir. Güvenli bir ortam sağlamak için, risklerin çeşitlerini ve sıklığını ve bunları azaltmak veya daha da iyisi ortadan kaldırmak için çözümleri anlamamız gerekir. Gençler çevrimiçi ortamda karşılaşılan riskler konusunda daha genç kullanıcılar için daha güvenli bir internet yaratmanın yolları ile ilgili önemli miktarda araştırma yapılmıştır. Çevrimiçi gençlerin karşılaştığı risklerden biri de siber zorbalık veya çevrimiçi mağduriyettir: yani elektronik iletişim şekillerini kullanan zorbalık veya taciz. Siber zorbalığın bazı örnekleri açıkça tanımlanabilirken diğerleri daha azdır. Siber kelimenin mağdurunu korkutmak için kullandığı dil ve taktiklerin cezai bir suç olduğunun açık işareti olduğu durumlarda olabilir, bazı durumlarda ise yalnızca bir şahsın kötü davranışlarından kaynaklanır. Siber zorbalık, genellikle eylemin tekrarını gerektirir. Siber zorbalığı yaygınlaştırma konusunda, özellikle geleneksel zorbalığa kıyasla açık bir anlaşma eksikliği var ve bu, yaygınlığı hakkındaki istatistikleri etkiliyor. İnternetteki siber zorbalığa hitap etmenin bir yolu, okul zorbalığı ve siber zorbalık arasındaki bağlantıyı kullanmaktır. Okul zorbalığına, gençlerin sahip oldukları ve birbirlerine karşı olan ilişkileri ve tutumları geliştirmeye çalışan girişimler denir. Bu tür girişimleri, çevrimdışı zorbalığa karşı koymak için potansiyel olarak etkili önleme tedbirleri olarak düşünülmekte ve çevrimiçi zorbalığa karşı koymada da yararlı olabilirler. Gençler ve yetişkinler genellikle çevrimiçi mağduriyet konusunda farklı yorumlara sahiptir. Yetişkinler bazı eylemleri bir şekilde tedavi etme eğilimi gösterirken, gençler aynı örnekleri akranları arasında normal bir etkinlik olarak açıklayabilir, ancak bunlar çevrimdışı bir sorunla başlar. Okullar, okul çapında bir zorbalık önleme programının oluşturulmasını kolaylaştıracak politikalar oluşturur ve bu programlar tipik olarak etkinliklerinin periyodik değerlendirmelerini içerir. Başarılı ve etkili programlar, bireysel öğrencilerden ve sınıflardan, eğitimcileri ve öğrencileri birleştiren zorbalık karşıtı takımlara kadar, okulda her seviyede zorbalık karşıtı stratejileri teşvik etmek için çalışır. Çoğu genç, utanç yüzünden çevrimiçi olarak karşılaştıklarında yetişkinleri dahil etmeme

eğiliminde oldukları için, ebeveynlerin ve eğitimcilerin, gençlerin zorluklarla karşılaşabileceğini belirtmek için dikkat etmeleri gereken işaretlerden haberdar edilmesi gerekir. Bu nedenle, kurslar ve bilgilendirici görüşmeler genellikle okullarda veya yerel konseyler tarafından organize edilirken, diğer etkin yöntemler filtreleme ve güvenlik duvarı teknolojilerini içerir. Buna ek olarak, internet erişimi sağlayan şirketlerin kullanıcıları için daha güvenli çevrimiçi ortamlar sağlamaları, dolayısıyla çevrimiçi riskleri ele almanın bir başka yolunu teşvik etmeleri önerilir. Gençlerin daha proaktif olarak çevrimiçi mahremiyetlerini korumaları durumunda, internetin oluşturduğu risklerin birçoğu azaltılabilir. Kişisel bilgilerin çevrimiçi olarak açığa çıkmasına daha az istekli olacak şekilde eğitilmeleri ve gizliliklerini nasıl yöneteceklerini bilmeleri gerekir; Bu tür eğitim, özellikle genç yaşta itibaren okullarda önemlidir. Ebeveynler ve çocukları arasındaki nesil boşluğu nedeniyle, birbirlerine güven duymalarını engelleyebilecek ve dolayısıyla çevrimiçi riskin etkili bir şekilde kontrol altına alınmasına neden olabilecek bir yanlış anlama olasılığı bulunmaktadır. Bu nedenle, gençlerle yetişkinler arasındaki iletişim teşvik edilmelidir; siber güvenlikle ilgili diyaloga girmek, boşluğu hafifletmeye ve güvenlik tedbirlerini geliştirmeye yardımcı olabilir. Bu tür diyaloglar aynı zamanda gençleri ebeveynlerini çevrimiçi olan kaynaklar ve web siteleri konusunda eğitmeye teşvik edebilir, Yarın dünyanın liderleri arasında internet güvenlik tedbirlerini tartışmak çok önemlidir. Web'in sağladığı yararlar modern kültürümüzün bir parçasıdır ve birçok teknolojik ilerlememizin gençlerin kendilerinin güvenliği konusunda geri tepmesine izin vermemeliyiz

. E GÜVENLİK MÜFREDATIMIZ HAKKINDA

- Medya okur-yazarlığı ve bilişim derslerinde internet kullanımı ile ilgili içerik güncel ve teknolojik gelişmeler ışığında güncellenmiştir .
- Çocuklarda bilinçli ve güvenli internet kullanımına dair bilgi, beceri ve tutumların geliştirilmesi için seminerler düzenlenmektedir .
- Türkçe, Fen Bilimleri vb ilgili derslerde uygun şekilde işlenmesi sağlanmaktadır .
- Ders müfredatlarına sosyal medya başta olmak üzere internetin bilinçli kullanımı ile ilgili konuların yenilenen bilgilerle güncellenmesi okul BİT koordinatör öğretmeni tarafından sağlanmıştır .
- Fatih projesinin yürütülmesi ve sürdürülmesi aşamasında teknolojinin etkili ve güvenli kullanımlarının sağlanması için BTK tarafından güvenli internet ağı mevcuttur .
- MEB'e bağlı okullarda elektromanyetik kirliliğe ve internet güvenliğine önem verilmektedir.

ÇOCUK VE ERGENLERE YÖNELİK e GÜVENLİK ÖNLEMLERİ

- Aileye yönelik çocuk ve ergenlere denetimli, sınırlı ve amaçlı kullanım sağlayabilmeleri ile ilgili bilinçlendirme çalışmaları yapmaktayız .
- İnternetin güvenli kullanımı ile ilgili paketlerin tanıtım ve yaygınlaşmasını sağlamak devlet politikasıdır .
- Evlerde limitli internet paketlerinin kullanımını teşvik etmek için rehberlik yapılmaktadır .
- Kullanım farkındalığına yönelik uygulamalar geliştirmek için derslerde bu konuya öncelik verilmektedir .
- Ebeveynleri denetim yolları ve teknolojik imkânları ile ilgili bilinçlendirmek ve gerekli uygulamaları geliştirmek ve yaygınlaştırmak için üniversiteden akademisyenlerden yardım alınmaktadır.

OKULUMUZDA FOTOĞRAF YADA VİDEO ÇEKİMİ VE YAYINLANMASI

1. Okul idaresi tarafından görevli kılınanlar haricindeki kişiler tarafından ve öğrenci velilerinin bilmek istedikleri etkinlik ve programlar dışındaki zamanlarda , okul ve okul bahçesi sınırları içerisinde fotoğraf ve video çekimi yapılamaz. Bu yasak bir öğrencinin diğer bir öğrencinin fotoğraf ve videosunu çekmek istemesi durumunda da geçerlidir. 2. Okul idaresi tarafından görevlendirilen kişilerin çektiği fotoğraf ve videolar ancak Okulun resmi web adresinde ve sanal ortamlarında, ilgili öğrenci velisinin talep ve yazılı onayı ile yayınlanabilir. Öğrencisi için onay vermeyen velinin öğrencisi ile ilgili fotoğraf ve videolar yayınlanmaz. 3. Velisi tarafından fotoğraf ve video görüntülerinin çekilip yayınlanmasına onay verilmeyen öğrencilerin, çekim esnasında psikolojik baskı yaşamaması için tedbirler alınır. 4. Okul görevlileri tarafından yayınlanan resim ve videolarda öğrencilerin kişisel

bilgilerine kesinlikle yer verilmez. 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. (okullar bunun nasıl uygulanacağını ve başarılacağını listelemelidir) 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.