SELCEN HATUN ANAOKULU

OKUL GÜVENLİK PLANI ve GÜVENLİK POLİTİKAMIZ

 Okul Güvenlik Politikaları hızla gelişmektedir, çünkü paydaşlar bugün internete okul binasından çok çeşitli şekillerde erişebilirler. Günlük yaşamımızın bir parçası olarak hepimiz teknolojilerle yaşıyoruz. Çocuklarımızın dijital teknolojilerle elde ettikleri fırsatları en iyi nasıl kullanacaklarını bildiklerinden emin olmak için, artık bunları nasıl kullanacaklarını bilmeli ve anlayabilmeliyiz. Bunun evde, okulda ya da arkadaşlarınızla ya da yalnız kaldığınız yerlerde mümkün olan en güvenli ortamda yapılmasını sağlamak için dikkat etmemiz gereken açık ve özlü bir Okul Politikamız vardır.

 Çocuklar ve teknoloji, günümüz dünyasında çoğu kez ayrılamaz. Web'in kullanımı artarken, güvenli kullanımı da önemlidir. Güvenli bir ortam sağlamak için, risklerin çeşitlerini ve sıklığını saptamak veya daha da iyisi ortadan kaldırmak için çözümler bulmamız gerekir. Çevrimiçi çocukların 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, çocukların 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.

 Çocuklar ve yetişkinler genellikle çevrimiçi mağduriyet konusunda farklı yorumlara sahiptir. Yetişkinler bazı eylemleri bir şekilde tedavi etme eğilimi gösterirken, çocuklar 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.

 Ağır internet kullanıcıları uygunsuz içerikle çevrimiçi karşılaşabilir; Çocuklar genellikle cinsel taciz veya cinsel içeriğe online olarak maruz kalma ile karşı karşıya kalabilir. World Wide Web' deki sınırsız içerik, çocukları istenmeyen cinsel içeriğin ve bilginin geniş bir koleksiyonuna götürebilir. Örnekler, cinsel konuşmalar, cinsel fotoğraflar gönderme veya talep etme veya istenmeyen cinsel bilgilerin ifşa edilmesini içerir. Ayrıca, istenmeyen pop-up' lar vasıtasıyla cinsel olmayan içerik için web' de gezinirken, çocuklar bazen müstehcen içerik veya cinsel imgelem / videolarla karşı karşıya kalırlar. E-posta dolandırıcılıkları alabilirler.

 İstenmeyen cinsel buluşmalarla uğraşmak için en yaygın önerilen strateji, çocukları bu tür sağlayıcıları engellemeye teşvik etmek veya onlara yardım etmek veya sorun yaşadıkları çevrimiçi forumdan ayrılmaktır. Çoğu çocuk, 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, ailelere kurslar ve bilgilendirici görüşmeler 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.

 Çocukların 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 çocuk yaştan 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, çocuklarla yetişkinler arasındaki iletişim teşvik edilmelidir; siber güvenlikle ilgili diyaloga girmek, boşluğu hafifletmeye ve güvenlik tedbirlerini geliştirmeye yardımcı olabilir. Bu tür diyaloglar aynı zamanda çocukların 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 çocukların kendilerinin güvenliği konusunda geri tepmesine izin vermemeliyiz.

E GÜVENLİK MÜFREDATIMIZ HAKKINDA

• Günlük eğitim akışlarımız internet kullanımı ile ilgili içerik güncel ve teknolojik gelişmeler ışığında güncellenmiştir

• Çocuklarda bilinçli ve güvenli internet kullanımına dair bilgi, beceri ve tutumların geliştirilmesi için çalışmalar düzenlenmektedir.

• Günlük akışta işlenen tüm konuların uygun şekilde işlenmesi sağlanmaktadır.

• Tüm etkinliklerde sosyal medya başta olmak üzere internetin bilinçli kullanımı ile ilgili konuların yenilenen bilgilerle güncellenmesi sınıf öğretmenleri ve rehber öğretmen tarafından sağlanmıştır.

• Okulumuzda internet güvenliğine önem verilmektedir.

1.Öğretmenler ,stajerler ve yardımcı hizmetler personeli cep telefonlarını öğrencilerin bulunduğu zaman ve ortamlarda kullanamazlar.

 2. Velilerle her yıl, eğitim öğretim yılı başında teknoloji kullanımı konusunda bilgi verme amaçlı toplantılar yapılır.

 3. Öğretmenlerle (eğitim öğretim başında, ortasında ve sonunda olmak üzere) yılda üç kez yapılan öğretmenler genel kurulunda okul güvenliği politikası hakkında değerlendirme amaçlı tartışmalar yapılır.

OKULUMUZDA FOTOĞRAF YADA VİDEO ÇEKİMİ VE YAYINLANMASI

1. Okul idaresi tarafından öğrenci velilerinin bilmek istedikleri etkinlik ve programlar dışındaki zamanlarda , okul ve okul bahçesi sınırları içerisinde fotoğraf ve video çekimi yapılamaz. Bu yasak bir velinin diğer bir velinin fotoğraf ve videosunu çekmek istemesi durumunda da geçerlidir.Okula kayıt esnasısında fotoğraf çekimi ve paylaşılması konusunda velilerden izin dilekçesi alınır.

 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.

 E-GÜVENLİK POLİTİKAMIZ

 Dijital teknolojiler okul çağı çocukları için de olağanüstü imkanlar ve fırsatlar sunuyor. Çocuklar da internet ortamının sağladıklarıyla bilgiye, eğlenceli oyunlara ve benzeri etkinliklere kolayca ve hızlıca erişim sağlayabiliyorlar. Ancak, dijital teknolojilerin sağladığı bu harika imkanların yanında, çocuğun zihinsel, ruhsal ve fiziksel saldırılarla, tuzaklarla karşılaşması tehlikesinin varlığı da hafife alınamaz bir gerçekliktir. Örnek vermek gerekirse internet ortamındaki bir çocuğun istem dışı da olsa karşısına çıkan bir reklamı izleme yoluyla ya da arama motoruna bilerek-bilmeyerek yazacağı yanlış bir kelime sebebiyle çocuğun merakını kışkırtan bir görsel onu zihinsel, duygusal ya da fiziksel olarak tehlikeye düşürecek ortamlara sürükleyebilir. Gün geçmiyor ki, bazı online oyunlar sebebiyle ebeveynleri korkutan, endişeye ve dehşete düşüren, ruhsal ya da fiziksel olarak mağdur olmuş bir çocukla ilgili bir haber duymamış olalım! Bu tehlikelerden çocuğu korumanın en emin yolu, onu internet ortamından tamamen uzak tutmaktır. Ancak çok hızlı gelişen dijital teknolojiler sebebiyle ve ne yazık ki, çocuğu internet ortamından tamamen uzak tutmak mümkün olmamakta, tamamen yasaklamak sorunu çözmemektedir. Kaldı ki çevresel etkenler ve ebeveyn tutumları sebebiyle internet ortamlarını tamamen yasaklamak ve erişimi engellemek imkansız bir hal almıştır. Bu sebeple çocuğu internet ortamının oluşturduğu tehlikelerden korumak için tamamen yasaklamaya çalışmaktan daha etkili tedbirler bulmak zorunluluğu vardır. Çocuğun söz konusu tehlikelerden kendisini koruması için çocuğa bilgi, bilinç ve davranış kazandırmaktan, bu hedef için çaba harcamaktan daha etkili bir yol kalmamaktadır. Bu gerçekler sebebiyle, okul politikası olarak öğrencilerimizi internet ortamlarının tehlikelerinden ve zararlarından koruyabilmek için ısrarlı ve kararlı bir şekilde uygulamalar gerçekleştirir ve gerekli, uygulanabilir yasaklar getiririz:

 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. Telekom buna yönelik güvenli internet paketi sunmaktadır.

• Evlerde limitli internet paketlerinin kullanımını teşvik etmek için rehberlik yapılmaktadır.

• Okul aile birliklerinin güçlendirilmesi ve teşvik edilmesi gereklidir.

• Güvenli internet paketi kullanımının yaygınlaşmasına yardımcı olunmalıdır.

• Aile içinde kullanılan bilgisayarların kullanıcıya göre farklı profiller oluşturmaya müsait olması ve güvenli internet hizmetinin de bu profillere göre farklı paketler ile sunulabilmesi gereklidir. Bununla ilgili çalışmalara başlanmıştır.

• 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 sınıf öğretmenlerimiz ve rehber öğretmenimizden yardım alınmaktadır.

 OKUL PERSONELİ

 Öğretmenlerimiz E Twinning mesleki gelişim portalından çevrimiçi ve online mesleki gelişim etkinliklerine katılmışlardır. 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 hepsi, çevrimiçi çevrimiçi davranışlarının okuldaki rolü ve itibarını etkileyebileceğinin farkına varacaktır. Mesleği veya kurumu tehlikeli durumuna düşürdüğü veya mesleki yeteneklerine güvenini kaybetmiş bir şeyin bulunduğu düşünülürse, hukuk, disiplin veya hukuki önlemler alınabilir. Okul çalışanların öğrencilerin yaşlarına ve yeteneklerine göre kullanması gereken yararlı çevrimiçi araçları kontrol etmelidir. 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 okulun çevrimiçi güvenlik (e-Güvenlik) politikasına ve beklentilerine yönelecektir. Evde ve okulda ebeveynlerle çevrimiçi güvenlik konusundaki işbirlikçi, yaklaşımı teşvik edilecektir. Evde güvenli İnternet kullanımı için gösteriler ve öneriler içeren ebeveyn eğitimleri sunma veya diğer iyi katılan etkinliklerde çevrimiçi güvenliğin vurgulanmasını içerebilir. ebeveyn eğitimleri, birlikte vakit geçirme ve spor günleri, gibi sosyal etkinlikler düzenleyeceklerdir. 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.

 Okulumuzda her yıl etkin ve kapsamlı veli desteği ile güvenli internet günü kutlanmıştır. Hafta boyunca seminerler, tanıtıcı afişler ve webinarlara etkin katılım sağlanmıştır. Okulumuz öğretmenleri e twinning portalında,safer ınternet facebook ,twitter hesaplarında paylaşım yapmışlardır. Daha Güvenli İnternet Merkezi (gim.org.tr) - Safer Internet Center'ın resmi sayfası.http://guvenlinet.org.tr/tr/ Güvenli Web (guvenliweb.org.tr) - çevrimiçi güvenlik konuları için farkındalık portalı. Güvenli Çocuk (guvenlicocuk.org.tr) - 13 yaşından küçük çocuklar için oyun ve eğlence portalı. Ihbar Web (ihbarweb.org.tr) - yasadışı içerik için telefon hattı. İnternet BTK (internet.btk.gov.tr) - İnternet ve BT yasası konusunda farkındalık portalı. SID Page (gig.org.tr) - Daha Güvenli İnternet Günü Türkiye'de resmi sayfası. Veli ve öğrencilere tanıtılmış buralardaki eğitici ebeveyn ve öğrenci bilgilendirici vidoları ,sunuları izlenmiştir. Okumuzda çeşiti web2 araçları kullanılarak sunular hazırlanmış, panolar ailelerle birlikte hazırlanmıştır. http://guvenlinet.org.tr/tr/ sayfasından bilgi amaçlı faydalanılmıştır.

Yeni teknolojiler konusunda çocuklar ve gençlerle doğrudan etkileşim sağlamak için

• bunları daha güvenli internet ile ilgili etkinliklere dahil edin.

• bu konudaki deneyimlerini görmek ve internet algılamalarını ölçmek.

• daha güvenli internet konusunda dijital okur-yazarlığı ve farkındalığı artırın.