



SELÇUKLU BELEDİYESİ İLKOKULU E-GÜVENLİK POLİTİKA BELGEMİZ

Bilgisayar ve internet, sadece erişkinler için değil; aynı zamanda çocuklar için de oldukça faydalı bir ortamdır. Çocukların, bir eğitim, eğlence ve iletişim aracı olarak bilgisayarlardan doğru ve etkin bir şekilde faydalanması adına birçok anne baba, çağa ayak uyma ve bilgiye daha çabuk ve etkin bir şekilde erişebilmeleri için çocuklarına bu tür imkânlar sunmak istemektedirler. Bilgisayar ve internet kullanımının çocuk ve gençlere sunduğu olumlu getirilerinin yanında, bu kullanımın olumsuz etkilerinin bulunduğu da her zaman göz önünde tutulmalıdır. Güvenli bir ortam sağlamak için, risklerin çeşitlerini ve sıklığını ve bunları azaltmak veya daha da, iyisi ortadan kaldırmak için çözümler aramamız gerekir. Gençler çevrimiçi ortamda karşılaşılan riskler konusunda daha genç kullanıcılar için daha güvenli bir internet yaratmanın yolları ile ilgili önemli miktarda araştırma yapılmıştır. Çocuklar ve gençler genel olarak, bilgisayar kullanırken veya internet üzerinde gezinirken bilgisayara, kendilerine ve ebeveynlerine verebilecekleri zararlar düşünmezler. Pek çok sorun ve riskle karşılaşır. Casus veya kötücül(malware) yazılımlarla karşı karşıya kalırlar. 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. Ağır internet kullanıcıları uygunsuz içerikle çevrimiçi karşılaşabilir; Gençler genellikle cinsel taciz veya cinsel içeriğe online olarak maruz kalma ile karşı karşıya kalabilir. World Wide Web'deki (WWW) sınırsız içerik, olgunlaşmamış gençleri istenmeyen cinsel içeriğin ve bilginin geniş bir koleksiyonuna

götürebilir.Örnekler, cinsel ilişki talepleri, 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, gençler bazen müstehcen içerik veya cinsel imgelem / videolarla karşı karşıya kalırlar.E-posta dolandırıcılıkları alabilirler. İstenmeyen cinsel buluşmalarla uğraşmak için en yaygın önerilen strateji, gençleri bu tür sağlayıcıları engellemeye teşvik etmek veya onlara yardım etmek veya sorun yaşadıkları çevrimiçi forumdan ayrılmaktır.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 çevrimiçi mahremiyetlerini korumaları durumunda, internetin oluşturduğu risklerin birçoğu azaltılabilir hatta ortadan kaldırılabilir.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

- SELÇUKLU BELEDİYESİ İLKOKULU, çevrimiçi güvenliğin (e-Güvenlik), bilgisayarlar, tabletler, cep telefonları veya oyun konsolları gibi teknolojiyi kullanırken, dijital dünyadaki çocukların ve yetişkinlerin korunması için vazgeçilmez bir unsur olduğuna inanmaktadır.
- SELÇUKLU BELEDİYESİ İLKOKULU, internetin ve bilgi iletişim teknolojilerinin günlük yaşamın önemli bir parçası olduğuna inanır. Dolayısıyla, riskleri yönetmeleri ve bunlara tepki vermek için stratejiler geliştirmenin yollarını öğrenmeleri için çocuklar desteklenmelidir.
- SELÇUKLU BELEDİYESİ İLKOKULU, eğitim standartlarını yükseltmek, başarıyı teşvik etmek, personelin mesleki çalışmalarını desteklemek ve yönetim işlevlerini geliştirmek için toplumun kaliteli İnternet erişimi sunma yükümlülüğüne sahiptir.
- SELÇUKLU BELEDİYESİ İLKOKULU, tüm çocukların ve personelin çevrimiçi olarak potansiyel zararlardan korunmasını sağlamakla sorumludur. • Bu politika, yöneticiler, öğretmenler, destek personeli, çocuklar ve ebeveynler için hazırlanmıştır. • 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 için de geçerlidir.

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 kullanımını 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.

CEP TELEFONU KULLANIMI

- Öğretmenler ve yardımcı hizmetler personeli cep telefonlarını öğrencilerin bulunduğu zaman ve ortamlarda kullanamazlar.
- Öğrenciler okula gelirken- öğrenci servisi aracı ile gelip gitmeleri ve servis görevlileri vasıtası ile öğrenciye ulaşma kolaylıkla mümkün olduğu için- cep telefonlarını getiremezler. Herhangi bir sebeple cep telefonlarını okula getirmek zorunda kalan öğrenciler cep telefonlarını Okul idaresinin gösterdiği yere ve ilgili görevliye, okul çıkışında almak üzere kapalı bir şekilde- teslim etmek zorundadırlar.Sınıfta herhangi bir öğrencinin cep telefonu bulundurması ve dolayısıyla kullanması yasaktır.
- Sınıf ortamında ve okul binası içinde cep telefonu bulundurma yasağını ihlal eden öğrencinin birinci ihlalde bir hafta, ikinci ihlalde iki hafta, üçüncü ihlalde dönem boyunca cep telefonuna okul idaresi tarafından (süre bitiminde iade edilmek üzere) el konulur. Kural ihlali durumunda uygulanacak bu yaptırımı öğrenci velisinin de desteklemesi için, eğitim öğretim yılı başında (ya da öğrencinin kaydı esnasında) yapılan yazılı sözleşme ile velinin kabulü sağlanır ve imzası alınır. Ayrıca veli kurallara uyulması esnasında güçlük çıkartırsa bu durum kolluk güçlerine bildirilir.
- Okul sınırları içerisinde herhangi bir öğrencinin wi-fi bağlantısına erişmesine izin verilmez. Diğer ifadeyle öğrencinin herhangi bir yolla şifreyi elde edip kablosuz ağ bağlantısına bağlanması yasaktır. Bu yasağı ihlal ettiği tespit edilen öğrencinin cep telefonuna bir hafta için el konulur.
- Okul ve derslik sınırları içerisinde öğrenci tarafından cep telefonu sadece ders etkinliği uygulamaları esnasında, öğretmenin kontrolü altında ve ders aracı olarak kullanılabilir. Bu amacın dışındaki kullanımlara izin verilmez.
- Öğrenci cep telefon numarasının, öğrenci velisinin izin verdiği kişiler dışındakiler tarafından öğrenilmesine izin verilmez.
- Velilerle her yıl, eğitim öğretim yılı başında cep telefonu kullanımı konusunda bilgi verme amaçlı toplantılar yapılır.
- Öğretmenlerle (eğitim öğretim başında, ortasında ve sonunda olmak üzere) yılda üç kez yapılan öğretmenler genel kurulunda okul güvenliği ve dolayısıyla cep telefonu politikası hakkında değerlendirme amaçlı tartışmalar yapılır. Ülkenizde yasal

zorunluluk olup olmadığına bakılmaksızın, okulunuzda açık bir fotoğraf ve imaj politikası olduğundan emin olun.

OKULUMUZDA FOTOĞRAF YADA VİDEO ÇEKİMİ VE YAYINLANMASI

- Okul idaresi tarafından görevli kılanlar 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.
- 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.
- Velisi tarafından fotoğraf ve video görüntülerinin çekilip yayınlanmasına onay verilmeyen öğrencilerin, çekim esnasında psikolojik baskı yaşamaması için tedbirler alınır.
- 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 gerçekleştirilecektir. 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.

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.

E-GÜVENLİK POLİTİKAMIZ

Digital 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, digital teknolojilerin sağladığı bu harika imkanların yanında, çocuğun zihinsel, ruhsal ve fiziksel saldırılarla, tuzaklarla karşılaşması tehlikesinin varlığı da hafife alınamaz bir

gerçeklidir. 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 pornografik bir siteye girmesi mümkündür ya da 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! Yukarıda kısaca söz edilmiş olan tehlikelerden çocuğu korumanın en emin yolu, onu internet ortamından tamamen uzak tutmaktır. Ancak çok hızlı gelişen digital 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. Öncelikle ifade etmek gerekir ki, dijital teknolojilerin sahip olduğu imkanlar sebebiyle alınabilecek hiç tedbir çocuğu yukarıda sözü edilen tehlikelerden yüzde yüz oranında koruyamayacaktır. Dolayısıyla 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.
- Gençlerin aktif olarak katılacağı sosyal projelerin arttırılmasına ihtiyaç vardır.
- 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.

OKUL PERSONELİ Tüm öğretmenlerimiz Hizmetiçi eğitim olarak İnternet Güvenliği eğitimlerine katılmaktadırlar. Muammer AKKUŞ European Schoolnet Academy tarafından eSafety Label belgesini almıştır. Yine e Twinning mesleki gelişim portalından çevrimiçi ve online mesleki gelişim etkinliklerine katılmışlardır. Sena KIZILÖZ KAYA , bu konuda M.E.B. tarafından düzenlenen hizmetiçi eğitim etkinliğine de katılmıştır ve personele eğitim de vermektedir. Ayrıca pandemi dolayısıyla yüzyüze eğitim verilemediğinden tüm öğrenci ve velilerin katılabildiği çevrimiçi e-güvenlik eğitimleri yine Sena KIZILÖZ KAYA tarafından verilmektedir. 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 temelde çeşitli şekillerde sağlanacaktır. Çalışanların hepsi, 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. Filtreleme sistemlerini yönetme veya BİT kullanımını izleme sorumluluğu taşıyan personelin üyeleri, Liderlik Ekibi tarafından denetlenecek ve sorunları veya endişeleri bildirmek için açık prosedürlere sahip olacaklardır. 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, bilgilendirme mektupları, 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. Güvenli İnternet Günü Okulumuzda 2020 ve 2021 yılında etkin ve kapsamlı veli desteği ile güvenli internet günü uzaktan bağlantılarla ve kısmi yüzyüze etkinliklerle kutlanmıştır. Hafta boyunca seminerler, tanıtıcı afişler ve webinarlara etkin katılım sağlanmıştır. Ayrıca müdür yardımcımız Muammer AKKUŞ tarafından hazırlanan kodlama çalışmaları öğrencilere evlerinde yaptırılmış okul web sayfasında yayınlanmıştır. Okulumuz öğretmeni(Türkan DEMİREL) e twinning portalında, safer internet SİD hesaplarında paylaşım yapmışlardır. Daha Güvenli İnternet Merkezi (gim.org.tr) - Safer Internet Center'ın resmi sayfası.<http://guvenlinet.org.tr/tr/> Güvenli Çocuk (guvenlicocuk.org.tr) - 13 yaşından küçük çocuklar için oyun ve eğlence portalı. İhbar Web (ihbarweb.org.tr) - yasadışı içerik için telefon hattı. İnternet BTK (internet.btk.gov.tr) - İnternet ve BT yasası konusunda farkındalık portalı. Güvenli Web (guvenliweb.org.tr) - çevrimiçi güvenlik konuları için 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 çeşitli web2 araçları kullanılarak sunular hazırlanmış, panolar ailelerle birlikte hazırlanmıştır. <http://guvenlinet.org.tr/tr/> sayfasından bilgi amaçlı faydalanılmıştır.



SELÇUKLU MUNICIPALITY PRIMARY SCHOOL OUR E-SECURITY POLICY

Computers and the internet are not just for adults; They are also a very useful environment for children. Many parents want to offer such opportunities to their children so that they can use computers as an education, entertainment and communication tool in a correct and effective way to keep up with the times and access information more quickly and effectively. In addition to the positive benefits of computer and internet useage for children and young people, it should always be kept in mind that this useage has negative effects. To maintain a safe environment, we need to look for the types and frequency of risks and solutions to reduce them or eliminate them. A considerable amount of research has been done on the risks faced in the teens online environment on ways to create a safer internet for younger users. Children and adolescents generally do not think about the harm they could cause to the computer, themselves and their parents while using the computer or surfing the internet. . They face many problems and risks. They are faced with spyware or malware. One of the risks faced by online teens is cyberbullying or online victimization: that is, bullying or harassment using forms of electronic communication. Some examples of cyberbullying are clearly identifiable while others are less. It may be in situations where the language and tactics the cyber word uses to frighten its victim is a clear sign of a criminal offense. In some cases, it is only caused by a person's bad behavior. Cyberbullying often requires repetition of action. There is a lack of clear agreement on spreading cyberbullying, especially compared to traditional bullying, and this affects statistics on its prevalence. One way to address cyberbullying on the internet is school bullying. School bullying is called initiatives that try to improve relationships and attitudes that young people have and towards each other. Such attempts can potentially be used to counter offline bullying. They are considered effective prevention measures and can also be useful in countering online bullying. Teens and adults often have different interpretations of online victimization. While adults tend to treat certain actions in some way, young people may explain the same examples as a normal activity among their peers, but these start with an offline problem. Schools establish policies that facilitate the establishment of a school-wide bullying prevention program, and these programs typically include periodic evaluations of their activities. Successful and effective programs work to promote anti-bullying strategies at all levels at school, from individual students and classes to anti-bullying teams that unite educators and students. Heavy internet users may encounter inappropriate content online; Teens can often face sexual harassment or exposure to sexual content online. Unlimited content on the World Wide Web (WWW) can lead immature teens to a large collection of unwanted sexual content and information. Examples include requests for sexual intercourse, sexual conversations, sending or soliciting sexual photos, or disclosing unwanted

sexual information. Also, when surfing the web for non-sexual content via unwanted pop-ups, teens are sometimes confronted with sexually explicit content or sexual imagery / videos. The most common recommended strategy for dealing with unwanted sexual encounters is to encourage or help teens to block such providers or leave the online forum where they have trouble. Most teens tend not to involve adults when they meet online because of embarrassment, so parents and educators may face difficulties for teens. Therefore, courses and informational talks are often organized in schools or by local councils, while other effective methods include filtering and firewall technologies. In addition, it is recommended that companies providing internet access provide safer online environments for their users, thereby promoting another way to address online risks. Many of the risks posed by the internet can be reduced or even eliminated if teens protect their privacy online. They need to be trained to be less willing to reveal personal information online and know how to manage their privacy; this type of education is especially important in schools from a young age. Because of the gap, there is a possibility of misunderstanding that could prevent them from trusting each other and thus lead to effective control of online risk. Therefore, communication between young people and adults should be encouraged; engaging in a dialogue on cybersecurity can help alleviate the gap and improve security measures. Such dialogues can also encourage young people to educate their parents about resources and websites that are online. Discuss internet safety measures among the world's leaders tomorrow is very important. The benefits of the web are part of our modern culture, and we shouldn't let our many technological advances backfire on the safety of young people themselves.

ABOUT OUR E SECURITY CURRICULUM

- SELÇUKLU MUNICIPALITY İLKOKULU believes that online security (e-Security) is an indispensable element for the protection of children and adults in the digital world when using technology such as computers, tablets, mobile phones or game consoles.
- SELÇUKLU MUNICIPALITY İLKOKULU believes that the internet and information communication technologies are an important part of daily life. Therefore, children should be supported to learn how to manage risks and develop strategies to react to them.
- SELÇUKLU MUNICIPALITY PRIMARY SCHOOL has the obligation to provide quality internet access to the society in order to raise the educational standards, encourage success, support the professional work of the staff and improve management functions.
- SELÇUKLU MUNICIPALITY İLKOKULU is responsible for ensuring that all children and staff are protected from potential harm online.
- This policy has been prepared for administrators, teachers, support staff, children and parents.
- This policy applies to internet access and use of information communication devices, including personal devices; It also applies to school-provided devices for remote use, such as laptops, tablets or mobile devices on which children, staff or other persons work.

SAFETY MEASURES FOR CHILDREN AND ADOLESCENTS

- We carry out awareness-raising activities for children and adolescents in the family so that they can provide controlled, limited and purposeful use.
- It is the government policy to promote and disseminate packages related to the safe use of the internet.
- Guidance is provided to encourage the use of limited internet packages in homes.
 - This subject is prioritized in lessons in order to develop applications for usage awareness.
- To raise awareness of parents about control methods and technological possibilities and to develop and spread the necessary applications. Getting help from academics from the university.

MOBILE PHONE USE

- Teachers and services staff cannot use their mobile phones when students are present.
- Students cannot bring their mobile phones while coming to the school - as it is easily possible to come and go by the student bus and reach the student through the service staff. Students who have to bring their mobile phones to the school for any reason are obliged to hand over their mobile phones to the place indicated by the school administration and to the relevant officer, in a closed form to collect them after the school.
- A student who violates the prohibition of having mobile phones in the classroom and in the school building will be confiscated by the school administration (to be returned at the end of the term) for one week in the first violation, two weeks in the second violation, and during the third term. In order for the parents of the student to support this sanction to be applied in case of violation of the rules, the parents' acceptance and signature is obtained with a written agreement made at the beginning of the academic year (or during the registration of the student). In addition, if the parents have difficulties in complying with the rules, this situation is reported to the law enforcement authorities.
- No student is allowed to access the wi-fi connection within the school boundaries. In other words, it is forbidden for the student to obtain the password and connect to the wireless network connection in any way. The mobile phone of the student who is found to have violated this ban is confiscated for a week.
- Within the boundaries of the school and classroom, the mobile phone can only be used by the student during the lesson activities, under the control of the teacher and as a lesson tool. Uses other than this purpose are not permitted.
- A student's mobile phone number is not allowed to be learned by anyone other than those permitted by the parent of the student.
- Meetings are held with parents every year at the beginning of the academic year to inform them about the use of mobile phones.
- Discussions are held with teachers (at the beginning, middle and end of education) three times a year on teachers' general assembly about school safety and therefore mobile phone policy. Regardless of whether there is a legal requirement in your country, make sure that your school has a clear photography and image policy.

PHOTOGRAPHY OR VIDEO MAKING AND PUBLISHING AT OUR SCHOOL

- No photographs and videos can be taken within the boundaries of the school and schoolyards by persons other than those assigned by the school administration and at times other than the activities and programs that parents of students want to know. This prohibition also applies if a student wishes to take photos and videos of another student.
- The photographs and videos taken by the persons assigned by the school administration can only be published on the official web address of the School and on the virtual environment, upon the request and written approval of the parents of the relevant student. Photos and videos about the student of the parent who does not give consent for the student are not published.
- Measures are taken to ensure that students who are not approved for taking and broadcasting photographs and videos by their parents do not experience psychological pressure during shooting.
- Students' personal information is never included in the pictures and videos published by school officials. Students will ask permission from a teacher before preparing or responding to a video conference call or message. Videoconferencing will be supervised appropriately for the students' age and ability. (Schools should list how to implement and achieve this) Parents and caregivers consent will be obtained before children participate in videoconferencing activities. Video conferencing will take place through formal and approved communication channels, following a robust risk assessment. Only main administrators are granted access to video conference administration areas or remote control pages. Unique login and password information for trained video conferencing services will only be provided to staff members and will be secured.

MANAGING THE SCHOOL WEBSITE

- Contact information on the website will be school address, e-mail and telephone number. Personal information of staff or students will not be published.
- The School Principal will take overall publication responsibility for published online content and ensure that the information is accurate and relevant.
- The website will comply with the school's publication guidelines, including accessibility, respect for intellectual property rights, privacy policies, and copyright.
- E-mail addresses will be carefully posted online to avoid spam mails.
- Student work will be published with the permission of the students or their parents. • The administrator account of the school website will be protected by appropriately encrypted with a strong password.
- The school will post information about protection on the school website for members of the community, including online safety.

OUR E-SECURITY POLICY

Digital technologies also offer extraordinary opportunities and opportunities for school-age children. With the help of the internet environment, children can easily and quickly access information, fun games and similar activities. However, in addition to these wonderful opportunities provided by digital technologies, the danger of the child encountering mental,

spiritual and physical attacks and traps is an inestimable reality. For example, it is possible for a child in the internet environment to enter a pornographic site by watching an advert that appears unintentionally or because of a wrong word that he will knowingly or unknowingly type in the search engine, or a visual that provokes the child's curiosity may endanger him mentally, emotionally or physically. it can drag the environment. Day after day, let's not hear a news about a child who has been physically or mentally victimized because of some online games that scared, anxious and terrified parents!

The safest way to protect the child from the dangers briefly mentioned above is to keep him completely out of the internet environment. However, due to very fast developing digital technologies and unfortunately, it is not possible to keep the child away from the internet environment completely, and banning it completely does not solve the problem. Moreover, due to environmental factors and parental attitudes, it has become impossible to completely ban internet environments and prevent access. For this reason, in order to protect the child from the dangers posed by the internet environment, it is imperative to find more effective measures than trying to ban it completely. First of all, it should be stated that no measures that can be taken due to the possibilities of digital technologies will not be able to protect the child from the dangers mentioned above by one hundred percent. Therefore, there is no more effective way to protect the child from these dangers than to gain knowledge, consciousness and behavior, and to strive for this goal. Due to these facts, as a school policy, we persistently and decisively implement practices and impose necessary and enforceable prohibitions in order to protect our students from the dangers and harms of the internet environment.

E-SAFETY MEASURES FOR CHILDREN AND ADOLESCENTS

- We carry out awareness raising activities for children and adolescents in the family so that they can provide controlled, limited and purposeful use.
- It is the government policy to ensure the promotion and widespread use of packages related to the safe use of the internet. Telecom offers a secure internet package for this.
- Guidance is provided to encourage the use of limited internet packages in homes. • Parent-teacher unions should be strengthened and encouraged.
- There is a need to increase the social projects in which young people can actively participate.
- It should be helped to spread the use of secure internet package.
- The computers used in the family should be able to create different profiles according to the user and secure internet service should be offered with different packages according to these profiles. Studies on this have been started.
- This subject is prioritized in lessons in order to develop applications for usage awareness.

SCHOOL STAFF, All our teachers participate in Internet Security trainings as in-service training. Muammer AKKUŞ has received the eSafety Label certificate from the European Schoolnet Academy. They also participated in online and online professional development activities from e Twinning professional development portal. Sena KIZILÖZ KAYA, M.E.B. She also participated in the in-service training event organized by Ş. and provides training for

the staff. In addition, since face-to-face training cannot be provided due to the pandemic, online e-security trainings, which all students and parents can attend, are also provided by Sena KIZILÖZ KAYA. The online safety (eSafety) policy will be formally provided and discussed for the participation of all employees, and strengthened and emphasized as part of our protection responsibility. Staff will be aware that Internet traffic can be monitored and tracked to a single user. Discretion and professional behavior are required when using school systems and devices.

All members of staff will be provided with up-to-date and appropriate staff training on safe and responsible Internet use in a variety of ways on a regular basis, professionally and personally. All employees will realize that their online behavior can affect their role and reputation at school. Legal, disciplinary or legal measures can be taken if it is thought that something is found that puts the profession or institution in a dangerous position or has lost confidence in their professional abilities. Members of staff with responsibility for managing filtering systems or monitoring the use of ICT will be overseen by the Leadership Team and have clear procedures for reporting issues or concerns. School staff should check useful online tools that students should use according to their age and abilities.

It recognizes that parents / caregivers have an important role to play so that children can become reliable and responsible users of the internet and digital technology. Parents' attention will be directed to the school's online safety (eSafety) policy and expectations on the newsletters, briefing letters, school prospectus and school website. A collaborative approach to online safety with parents at home and school will be encouraged. It may include providing parent education with demonstrations and recommendations for safe Internet use at home, or emphasizing online safety at other well-attended events. They will organize social activities such as parent education, spending time together and sports days. As part of the School Agreement, parents will be required to read online safety information. Parents will be encouraged to read the School Acceptable Use Policy and discuss its effects with their children. Information and guidance for parents on online safety will be provided to parents in a variety of formats. Parents will be encouraged to role model positive behaviors for their children online. Safe Internet Day In 2020 and 2021, our school celebrated the safe internet day with effective and comprehensive parent support with remote connections and partial face-to-face activities.

Active participation was provided to seminars, promotional posters and webinars throughout the week. In addition, the coding studies prepared by our vice principal Muammer AKKUŞ were made by students at their homes and published on the school website. Our school teacher (Türkan DEMİREL) shared their shares on the twinning portal, on their safer internet SID accounts. Safer Internet Center (gim.org.tr) - The official page of Safer Internet Center.<http://guvenlinet.org.tr/tr/> Safe Child (guvenlicocuk.org.tr) - Games and entertainment for children under 13 portal. Ihbar Web (ihbarweb.org.tr) - hotline for illegal content. Internet BTK (internet.btk.gov.tr) - Awareness portal on Internet and IT law. Secure Web (guvenliweb.org.tr) - awareness portal for online security issues. SID Page (the.gig.org.t) - Safer Internet Day, the official sayfası. vel parents and students have been introduced around the educational and informative vidoe students in Turkey, presentations were followed. Presentations have been prepared using various web2 tools in our school, and boards have been prepared with families. The page <http://guvenlinet.org.tr/tr/> has been used for information purposes.

