

ŞEHİT MEHMET ALİ KÖRÜKÇÜ MESLEKİ VE TEKNİK ANADOLU LİSESİ

E-GÜVENLİK STRATEJİK PLANI

Gençler ve teknoloji, günümüz dünyasında çoğu kez ayrılamaz. Wen'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 çevrim içi ortamda karşılaşılan riskler konusunda daha genç kullanıcılar için daha güvenli bir internet yaratmanın yolları ile ilgili önemli miktarda araştırma yapılmıştır.

Çevrim içi gençlerin karşılaştığı risklerden biride siber zorbalık veya çevrim içi mağdur yani elektronik iletişim şekillerini kullanan zorbalık veya taciz. Siber zorbalığın bazı örnekleri 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, çevrim dışı zorbalığa karşı koymak için potansiyel olarak etkili önleme tedbirleri olarak düşünülmekte ve çevrim içi zorbalığa karşı koyma 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 çevrim dışı bir sorunla başlar. Okullar, okul çapında bir zorbalık önleme programının oluşturulmasını kolaylaştıracak politikalar oluşturur ve bu programlar tipik olarak etkinliklerinin periyodik değerlendirilmelerini içerir. Başarılı ve etkili programlar, bireysel öğrencilerden ve sınıflardan , eğitimcileri ve öğrencileri birleştiren zorbalık karşıtı takımlara kadar, okulda her seviyede 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 Web 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 pornografik vasıtasıyla cinsel olmayan içerik için 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 çevrim içi forumdan ayrılmaktır. Çoğu genç, utanç yüzünden çevrim içi olarak



karşılaştıklarında yetişkinleri dahil etmeme eğiliminde oldukları için, ebeveynlerin ve eğitimcilerin ,gençleri zorluklarla karşılaşılabileceğini 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 erişimini sağlayan şirketlerin kullanıcıları için daha güvenli çevrim içi ortamlar sağlamaları ,dolayısıyla çevrim içi riskleri ele almanın bir başka yolunu teşvik etmeleri önerilir.

Gençlerin daha aktif olarak çevrimiçi mahremiyetlerini korumaları durumunda internetin oluşturduğu risklerin birçoğu azaltılabilir. Kişisel bilgilerin çevrimiçi olarak açığa çıkmasına daha az istekli olacak şekilde eğitmeleri ve gizliliklerini nasıl yöneteceklerini bilmeleri gerekir bu tür eğitim 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, gençlere yetişkinler arasındaki iletişim tedbirlerini geliştirmeye yardımcı olabilir. Bu tür diyaloglar ayrı zamanda gençleri ebeveynleri çevrimiçi olan kaynaklar 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 bir çok teknolojik ilerlememizin gençlerin kendilerini güvenliği konusunda geri tepmesini izin vermemeliyiz.

E-GÜVENLİK MÜFREDATIMIZ HAKINDA

Medya okur-yazarlık 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 ,sağlık bilgisi ,fen bilimleri ve benzeri ilgili derslerle uygun şekilde işlenmesi sağlanmaktadır.

Ders müfredatlarına sosyal medya başta olmak üzere internetim bilinçli kullanımı ile ilgili konuların yenilenen bilgilerle güncellenmesi okul müdür yardımcısı tarafından sağlanmıştır.

Milli eğitim bakanlığı 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 için ile ilgili bilinçlendirme çalışmaları yapmaktayız.

İnternetin güvenli kullanımı ile ilgili paketlerin tanıtım ve yaygınlaşmasını sağlamak devlet politikasıdır.

Evlerde limitli internet paketlerinin kullanımları teşvik etmek için rehberlik yapmaktadır.

Ebeveynleri denetim yolları ve teknolojik imkanları ile ilgili bilinçlendirmek ve gerekli uygulamaları geliştirmek ve yaygınlaştırmak için üniversiteden akademisyenlerden yardım alınmaktadır.

CEP TELEFONU KULLANIMLARI

Bu sebeple;

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

2.Öğrenciler okula gelirken –öğrenci servisi aracı ile gelip gitmeleri ve servis görevlileri vasıtası ile öğrenciye ulaşmak kolaylıkla mümkün olduğu için –cep telefonlarını getiremezler. Her hangi bir sebeple cep telefonlarını okula getirmek zorunda kalan öğrenciler cep telefonlarını teslim etmek zorundadırlar. Sınıfta her hangi bir öğrencinin cep telefonu bulundurması dolayısıyla kullanması yasaktır.

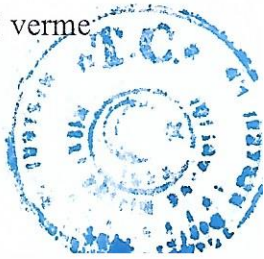
3.Sınıf ortamında ve okul binasında işinde cep telefonu bulundurma yasağını ihlal eden öğrencinin birinci ihlalde bir hafta ,ikinci ihlalde iki hafta üçüncü ihlalde dönem boyunca cep telefonunla okul idaresi tarafından (süre bitiminde iade edilmek üzere) el konulur . kural ihlali durumunda uygulanacak 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 .

4.Okul sınırları içerisinde her hangi bir öğrencinin bağlantısına erişmesine izin verilmez . diğer ifade ile her hangi bir yolla şifreyi elde edip kablosuz ağa bağlantısına bağlanması yasaktır. Bu yasağı ihlal ettiği tespit edilen öğrencilerin cep telefonunda bir hafta için el konulur.

5.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.

6.Öğrenci cep telefonu numarasını ,öğrenci velisinin izin verdiği kişiler dışındakiler tarafından öğrenilmesi izin verilmez.

7.Velilerle her yıl ,eğitim öğretim yılı başında cep telefonu kullanımı konusunda bilgi verme amaçlı toplantılar yapılır.



8.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.

OKULUMUZDA FOTOĞRAF YA DA VIDEO ÇEKİMİ VE YAYINLANMASI

1. Okul idaresi tarafından görevli kılınanlar haricindeki kişiler tarafından ve öğrenci verilerin bilmek istedikleri etkinlik ve programlar dışındaki zamanlar, okul ve okul bahçesi sınırları içerisinde fotoğraf ve video çekimi yapılamaz Bu yasak bir öğrencinin diğer bir öğrencinin fotoğraf ve videosunu çekmek istenmesi durumunda da geçerlidir.
2. Okul idaresi tarafından görevlendirilen kişilerin çektiği fotoğraflar ve videolar yayınlanmaz.
3. Velisi tarafından fotoğraf ve video görüntülerinin çekilip yayınlanmasına onay verilmeyen öğrencilerin; çekim esnasında psikolojik baskı yapmaması 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 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.

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 etkinliklerle kolaysa ve hızlıca erişim sağlayabiliyorlar. Ancak, dijital teknolojilerin sağladığı bu harika imkanların yanında, çocuğun zihinsel, ruhsal ve fiziksel saldırılara, 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 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 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 zorunluluđu vardır.

Öncelikle ifade etmek gerekir ki, dijital teknolojilerin sahip olduğu imkanlar sebebiyle alına bilecek hic tedbir çocuğu yukarda sözü edilen tehlikelerden yüzde yüz oranında koruyamayacaktır. Dolasıyla 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 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.

Okula aile birliklerinin güçlendirilmesi ve teşvik edilmesi gereklidir.

Gençlerin aktif olarak katılacağı sosyal projelerin arttırılmasına ihtiyaç vardır.

Güvenli internet paketi kullanımının yaygınlaşmasına yardımcı olmalıdır.

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 konulara öncelik verilmelidir.

OKUL PERSONELİ

Okulumuz personeli European Scholnet (www.eun.org) tarafından her yıl yapılan eğitimlere katılmaktadırlar Yine e TWİNNİNG mesleki gelişim portal dan 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 , internet trafiğinin izlenebileceği 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 olara, güvenli ve sorumlu İnternet kullanımı güncel ve uygun personel eğitimi, düzenli (en az yıllık) 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 personel üyeleri , Liderlik Ekibi tarafından denetlenecek ve sorunları veya endişeleri bildirmek için açık prosedürlere sahip olacaklardır. Okul çalışanların öğrencilerin yaşlarına ve yeteneklerine göre kullanılması gereken 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 İzah name ve okul MEB sitesinde okulun çevrimiçi güvenlik (e-Güvenlik) politikasına ve beklentilerine yönelecektir. Evde ve okulda ebeveynlere çevrimiçi güvenlik konusundaki işbirlikçi , yaklaşımı teşvik edilecektir. Evde güvenli internet 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 düzenleyecektir. Okul anlaşmasının bir parçası olarak ebeveynlerin çevrimiçi güvenlik bilgilerini okumaları istenecektir. Ebeveynler , Okula Kabul Edilebilir Kullanım Politikasını 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.

İNTERNET SİTESİ YAYIN EKİBİ KOMİSYONU



Bilişim Teknolojileri Öğretmeni

Hüseyin Seyhan DUYGU



Edebiyat Öğretmeni

Fadimana YETİŞ MEŞE



İngilizce Öğretmeni

Reyhan DOĞAN



OKUL MÜDÜRÜ

CEM YILMAZ