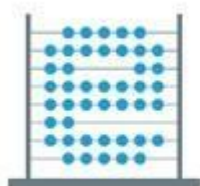


OSNOVNA ŠKOLA IVANA GUNDULIĆA



e-Škole

RAZVOJ SUSTAVA
DIGITALNO ZRELIH ŠKOLA
(II. FAZA)

PRAVILNIK O SIGURNOJ I ODGOVORNOJ UPOTREBI INFORMACIJSKO - KOMUNIKACIJSKE TEHNOLOGIJE u Osnovnoj školi Ivana Gundulića

Zagreb, lipanj 2023.

UVOD

SVRHA

Ovaj Pravilnik propisuje način prihvatljivog korištenja računala i IKT resursa škole s ciljem zaštite korisnika i sustava od malicioznog koda (računalni virusi), masovnih poruka (SPAM), raznih prijevara (SCAM), zaštite privatnosti, krađe podataka, uništenja podataka, krađe identiteta, zlostavljanja i drugih mogućih kriminalnih radnji.

Pravilnikom se propisuje pristojno ponašanje korisnika interneta i računalnih resursa, glede ponašanja prema drugim osobama, poštivanja osobnosti i privatnosti, te poštivanje autorskih prava.

Ovim pravilnikom se čuva trajnost i ispravnost strojne i programske opreme kao bi ista besprijekorno radila na opću korist i zadovoljstvo korisnika. Pravilnik neće sam po sebi onemogućiti pojavu nabrojanih i neželjenih pojava, ali će značajno doprinijeti u njihovom sprječavanju i smanjivanju istih.

PODRUČJE PRIMJENE

Ovaj Pravilnik se primjenjuje u Srednjoj školi Blato na sve resurse IKT opreme kao što su: računala, pisači, žična i bežična mreža, te svi drugi umreženi uređaji. Također, primjenjuje se na korištenje svih dostupnih servisa, e- pošte, e-matice, e-dnevnika, uredskih aplikacija, tražilica, društvenih mreža i drugih internet resursa i računalnih programa.

ODGOVORNOSTI I OVLAŠTENJA

Za primjenu i pridržavanje ovog pravilnika odgovorni su svi učitelji, stručni suradnici, administrativno i tehničko osoblje, djelatnici, administratori sustava i učenici. Sugestije za izmjene i dopune ovoga Pravilnika mogu predlagati svi na koje se isti odnosi.

OSNOVNE SIGURNOSNE ODREDBE

OSNOVNI POJMOVI

Korisnici IKT opreme su nastavnici, djelatnici, administratori sustava, učenici, roditelji i gosti u školi.

Osobe s posebnim zaduženjima:

- administrator imenika – odgovoran za održavanje LDAP imenika (AAI@eduHr)
- administrator resursa – odgovoran za raspodjelu resursa korisnicima
- administrator e-matice – odgovoran za administraciju e-matice
- administrator e-dnevnika – odgovoran za administraciju e-dnevnika
- operator e-matice – učitelji
- operator e-dnevnika – učitelji
- e-tehničar – odgovoran za cjelokupnu mrežu, računala i drugu periferiju, instalacije, održavanje, nadogradnje i rashodovanje opreme. Škola ima vlastitog e-tehničara i e-Škole tehničara kojeg je imenovala Županija kao osnivač.

IKT oprema u školi obuhvaća: računala, pisače, mrežnu opremu, programsku opremu, servise i resurse ministarstva, a kojima upravlja CARNET, kao i IKT opremu koja je u vlasništvu Škole.

- **Računala** dijelimo na višekorisnička i osobna. Višekorisnička su učenička računala u informatičkim učionicama i nastavnička u razredima, učenički tableti, te slobodna prijenosna računala, kao i tzv. "pametne ploče".
- **Pisači** su uređaji za ispis na papir, kopiranje i skeniranje.
- **Mrežu** tvore žična i bežična instalacija i komponente postavljena po cijeloj školi u svim razredima i uredima, te distribucijski komunikacijski ormari, kao fizički dio mreže, te ugrađeni protokoli i uređaji koji tvore logički dio mreže.
- **Programska oprema** obuhvaća operativne sustave, druge računalne programe bilo besplatne, kupljene ili osigurane od strane ministarstva, a služe za osnovni rad računala (OS), zaštitu računala te za potrebe poučavanja, istraživanja i poslovne svrhe.
- **Servisi i resursi ministarstva** pod nadzorom CARNET-a jesu svi internet mrežni resursi kao AAI@edu imenik, e-matica, e-dnevnik, e-pošta, web poslužitelji sa stranicama škole skole.hr, i drugo.
- **Servisi i resursi škole** jesu lokalni poslužitelji, zajednički diskovni prostor za pohranu, te drugi internet resursi koje škola plaća i daje na raspolaganje korisnicima.

Kritični resursi s osjetljivim podacima:

- **AAI@eduHr identitet** – poznat i kao 'imenik' ili 'LDAP'
- **e-matica** – evidencija svih učenika i nastavnika sa osobnim podacima, baza za e-dnevnik
- **e-dnevnik** – dnevnik aktivnosti, zapažanja i ocjena, po razredima, predmetima i učenicima

Sigurnosne odredbe

- Svi korisnici sustava su se dužni pridržavati ovog pravilnika.
- Sve važne zaporce sustava se drže zapisane u zapečaćenoj kuverti koja se čuva u sefu u tajništvu. Na kuverti mora pisati: „zaporse“, „Samo ravnatelj!“ i „Datum zadnje izmjene:“
U kuverti se nalaze sve „master“ zaporse koje su neophodne za pristup važnim djelovima sustava i resursima, obnovu drugih zaporki i slično. Ovlaštenje za pristup kuverti i održavanje sadržaja ima samo ravnatelj i tajnik škole.
- Sva školska IKT oprema se mora čuvati i koristiti pažljivo i na propisani način.
- Škola koristi tehničke mjere zaštite od računalnih napada, malicioznog koda, neželjenih poruka i slično u onoj mjeri koliko je to moguće. U tehničke mjere spadaju vatrozid, antivirusni programi, instalacija legalnih softvera, redovite nadogradnje i održavanje istih.
- Mehanizme zaštite osobnih podataka, a koji su pohranjeni na kritičnim mrežnim resursima (AAI@Edu, e-matica, e-dnevnik i drugi) postavlja, održava i nadzire CARNET. Pristup navedenim servisima i podacima je moguć prema strogo određenom sustavu dozvola i uloga svakog pojedinca u sustavu. Pristup se vrši upotrebom korisničkog imena i zaporse. U tom smislu, svi korisnici koji pristupaju ovim servisima, odgovorni su za čuvanje tajnosti podataka, te također čuvanje svojih pristupnih podataka od krađe i zlouporabe.
- Korisnici su dužni čuvati zaporse za pristup i pinove na način da ih nitko neovlašten ne može koristiti.
- Korisnici su također dužni periodično mijenjati zaporse na adresi: <https://login.aaiedu.hr/promjenazaporse/> pri čemu "jačina" zaporse mora zadovoljiti slijedeće uvjete: minimalno 8 znakova i sadržavati bar 2 znamenke i bar 2 slova.
- Nastavnicima, djelatnicima i učenicima je strogo zabranjeno davati vlastite zaporse i digitalne identitete drugim osobama.
- Svi djelatnici škole moraju potpisati izjavu o tajnosti podataka te se moraju pridržavati etičkih načela pri korištenju IKT-a.
- Svi nastavnici i zaposlenici škole su dužni koristiti službenu e-mail adresu oblika **ime.prezime@skole.hr** za službenu komunikaciju.
- Svi korisnici koji imaju AAI@edu identitet u slučaju zaborava zaporse, dužni su osobno doći u tajništvo škole i popuniti obrazac zahtjev za izdavanje nove zaporse. Zaporka se uručuje isključivo i osobno podnositelju zahtjeva.
- U slučaju u bilo kakvih nejasnoća kod korištenja servisa ili opreme, potrebno se konzultirati s osobama u školi koje su odgovorne za korištenje sustava ili djelova sustava: e-škole -tehničar, administratori škole i ravnatelj.
- Za upoznavanje korisnika sa svim izmjenama u načinima korištenja sustava, novim prijetnjama sigurnosti, odgovorne su osobe s posebnim zaduženjima (administratori, tehničari, ravnatelj i drugi) koje po definiciji prve saznaju za promjene i novosti nastale u sustavu. Načini prenošenja ovih informacija na korisnike mogu biti u cirkularnim pismom na papiru, e-mailom, objavom na školskim web stranicama, dijeljenim pretincima na OneDrive ili neposrednim prijenosom informacija na dogovorenom sastanku.

- Način korištenja i ovlasti za kritične resurse propisani su CARNET pravilima. Ravnatelj škole je dužan imenovati osobe s posebnim ovlastima kao administratore sukladno navedenim pravilima. Isključivo imenovani administratori imaju pristup ovim resursima. Oni unutar svojih ovlasti delegiraju ovlasti na operatore i korisnike pojedinih resursa.
- U tri kritična resursa se pohranjuju najosjetljiviji podaci učenika, nastavnika i djelatnika. Zaštita istih od nedozvoljenih uvida, kopiranja, izmjena i slično je prioritet. Odgovornost na zaštiti ovih podataka leži na administratorima i korisnicima. Odavanje pristupnih podataka, zaporki i tokena je najstrože zabranjeno. Neovlašteno ustupanje ili zlouporaba ovih podataka regulirana je zakonom.
- Održavanje imenika, e-matice i e-dnevnika vrše administratori i operatori na način kako je propisan uputama za svaki od pojedinih resursa od strane CARNET-a.

ŠKOLSKA IKT OPREMA I ODRŽAVANJE

Osnovni pojmovi

Školska mreža

Školska mreža se sastoji od žične i bežične infrastrukture. Sve učionice, kabineti i uredi su kablirani i imaju žične priključke na lokalnu mrežu i dalje na internet. Cijeli prostor škole je pokriven bežičnom mrežom, s naglaskom (jačim signalom i propusnošću) u učionicama i zbornici, te nešto slabijim signalom po hodnicima i drugim sporednim prostorima.

Detalji cjelokupne mrežne infrastrukture nalaze se u dokumentu "Projekt mrežne infrastrukture" (u daljnjem tekstu Projekt mreže) koji nije dio ovog pravilnika. Projekt mreže se redovito usklađuje s promjenama koje se u školi događaju na infrastrukturi, kako bi stanje u dokumentaciji bilo uvijek svježije što je važno za održavanje, izmjene i dogradnju mreže.

Školska računala

Školska računala su raspoređena na slijedeći način:

- **Računala nastavnika.**
U svakom razredu na nastavničkom stolu je stacionarno računalo (stolno ili prijenosno), koje je spojeno bežično ili kabelom na žičnu mrežu škole.
- **Računala u učionicama**
Informatička učionica ima 28 stolnih računala u informatičkoj učionici na prvom katu (za predmetnu nastavu), ? stolnih računala u informatičkoj učionici u prizemlju (za razrednu nastavu), i 200 tableta. Sva računala su spojena na lokalnu mrežu kabelima i/ili bežično.
- **Pametne ploče** su postavljene u ? učionica i umrežene kabelima na lokalnu mrežu.
- **Računala djelatnika** se nalaze u uredima djelatnih osoba: ravnatelj, tajnik, računovođa, psiholog, knjižničar.
- **Slobodna računala u zbornici** na korištenje nastavnicima
- **Prijenosna računala** su dodijeljena kao osobna računala nastavnicima u sklopu projekta eškole II faza.
- **Učenički tableti** u sklopu projekta Škola za život koriste učenici prema potrebi.

Pisači

Multifunkcijski uređaji za ispis, kopiranje skeniranje ili samo uređaji za ispis, nalaze se na više lokacija u školi, te su umreženi.

Projektori

Više učionica ima stacionarne projektore.

Komunikacijski ormari i oprema

- Infrastrukturna mrežna oprema je raspoređena na slijedeći način.
- Jedan veliki komunikacijski ormar BD1 u sobi uz ured ravnatelja.
- Manji komunikacijski ormar FD1 u učionici br. 10
- Manji distribucijski ormari EFD1, EFD2 i EFD3 u informatičkim učionicama
- Bežične komunikacijske točke u svim učionicama.

Postavljanje, instalacija i održavanje IKT opreme

- Jednom postavljena i podešena, oprema zahtjeva određeni nadzor, održavanje i popravljivanje.
- Većina infrastrukture, ne zahtjeva posebno održavanje tijekom eksploatacije jer je takve građe da uglavnom radi bez intervencija. U slučaju kvara, locira se neispravna komponenta i traži zamjena.
- Za opremu koju je montirao CARNET u sklopu projekta e-škole II faza, obavezno slijediti postupak popravka definiran od strane CARNET-a ili se postupi prema trenutnim uputama od helpdesk službe CARNET-a. S postupcima je upoznat e-tehničar.
- Ostalu mrežnu opremu u isključivom vlasništvu škole (EBD1, EFD1, EFD2, EFD3) e-tehničar održava kao je opisano u ovom pravilniku dolje.
- Sva računala u školi (stolna, prijenosna, tablete i pametne ploče) instalira, nadograđuje i održava e-tehničar. U slučaju kvara na računalima u vlasništvu CARNET-a (prijenosnici, tableti, pametne ploče) na popravak se upućuju prema postojećim uputama iz CARNET-a ili direktnim uputama iz helpdeska.
- Sva IKT oprema u vlasništvu škole za koju je potrebna usluga vanjskog servisa šalje se ili se poziva najbliži servis ili onaj servis s kojim škola ima ugovor o održavanju. Odluku o slanju opreme na servis donosi ravnatelj i e-tehničar na temelju međusobnih konzultacija.
- Za jednostavnije kvarove na opremi u vlasništvu škole rješive zamjenom komponenti, vrši e-tehničar.
- Odgovarajuće komponente se nabavljaju preko dostupnih web trgovina u republici Hrvatskoj.
- Preporuča se imati na zalihi nekoliko rezervnih komponenti kao što su miševi, tipkovnice, računalna napajanja, lampe za projektore, tzv. patch kabeli, hdmi, usb kabeli i drugo što praksa pokaže da je potrebno. Za rezervne komponente potrebno je osigurati mjesto za čuvanje, poželjno pod ključem (ormar, ladice i slično). O stanju zalihe i upotrebi komponenti i evidenciju vodi e-tehničar.
- Nabavka potrošnog materijala, tonera za ispis i papira dijelom je regulirana ugovorom o najmu, održavanju i isporuci potrošnog materijala sa dobavljačem. Manji ispisni uređaji koji nisu pod ugovorom održavanju, tonere se nabavlja standardnim postupkom nabave od raznih dobavljača. Radi trajnosti uređaja, preporučuje se nabava kvalitetnih tonera i tinti kao ih preporučuje proizvođač, a izbjegavati razne zamjenske opcije.

Rashodovanje dotrajale opreme

IKT oprema koja s vremenom dotraje i stavi se izvan upotrebe, potrebno ju je najprije prijaviti u rashod ukoliko je upisana u knjigu inventara ili osnovnih sredstava. Rashodovana oprema se skladišti na za tu svrhu određenom mjestu u školi. Kad se nakupi veća količina opreme, potrebno je pozvati tvrtku koja na području općine ili županije ima koncesiju za prikupljanje i odvoz elektroničkog otpada. Dokument o preuzimanju robe se trajno čuva kao dokaz o legalnom rješavanju elektroničkog otpada.

Generalne mjere zaštite IKT opreme

Da bi se sačuvao integritet strojne i programske opreme i sigurnost korisnika i da se olakša održavanje opreme sva računala u školi moraju biti instalirana kako je definirano u "Pravilniku za instalaciju i postavke školskih računala".

Osnovna načela su:

- Osnovna pravilo je da na svim računalima bude isti, po mogućnosti zadnji, uvijek ažurirani operativni sustav (OS). Odstupanje od ovog pravila je opravdano jedino tehničkim razlozima.
- **'Administrator resursa'** preuzima sa CARNET stranica odgovarajuće instalacijske datoteke operativnog sustava i drugih dostupnih alata kao i pripadajuće ključeve za aktivaciju i predaje e-tehničaru.
- **E-tehničar** vrši instalaciju računala prema "Pravilniku za instalaciju i postavke školskih računala".
- Strogo se zabranjuje upotreba softvera i ključeva suprotno licencnim pravilima. Zabranjuje se instalacija i upotreba ključeva na računala koja nisu vlasništvo škole.
- Strogo se zabranjuje dijeljenje ključeva bilo kojim trećim osobama. Administrator resursa i e-tehničar su jedine osobe koje smiju raspolagati s aktivacijskim ključevima.
- Na svim školskim računalima postaviti korisnički 'admin' račun zaključan zaporkom. Na svim računalima postavlja se ista admin zaporka. Samo e-tehničar je zna i čuva. Ova zaporka se također čuva kao 'master' zaporka u sefu u tajništvu u zapečaćenoj kuverti kako je ranije opisano. Dozvolu za upotrebu ove zaporke e-tehničar smije dati nastavniku informatike koji tada postaje odgovoran za čuvanje tajnosti iste.
- Admin zaporka se ne smije predati niti vanjskim servisima kad se računalo šalje na popravak. U tom slučaju se ako je moguće ta zaporka na tom računalu mijenja u neku privremenu prije slanja na servis ili se primjenjuje potpuna reinstalacija OS-a. Pri tome se postupa kao je opisano u pravilniku za instalaciju.
- Na svim multikorisničkim računalima se ugrađuje korisnički račun ('učenik' ili 'nastavnik') bez administratorskih prava i bez zaporke
- Dodatno se običnom korisniku naročito učeniku, blokira promjena svih vitalnih postavki
Detaljne upute su u 'Pravilniku o instalaciji i postavkama školskih računala'.

Evidencija školske IKT opreme

E-tehničar, u sklopu instalacija i nadogradnji, vodi evidenciju IKT opreme, prije svega računala. Svako računalo mora imati jedinstveno ime/naziv koji se nalazi u evidencijskoj listi, na naljepnici na kućištu računala i upisan u polje "Naziv računala" u samom OS-u kako bi se računalo identificiralo kroz sustav nadzora mreže. Detalji o načinu označavanja i vođenja evidencije opisani su u "Pravilniku za instalaciju i postavke školskih računala".

REGULIRANJE PRISTUPA IKT OPREMI

Pristup mreži

- Pristup bežičnoj mreži je strogo određen CARNET-ovim pravilima i tehnički moguć zahvaljujući osiguranoj infrastrukturi. Općenito, pristup bežičnoj mreži je moguć preko standardnih bežičnih mreža koje imaju nazive "Eskole" i "Eduroam"
- Eskole i Eduroam su standard na cijelom području Hrvatske, a "Eduroam" i Europe. Korisnici pristupaju svojim AAI@Edu identitetima, a prema uputama na CARNET stranicama i u "Projektu" ili uputama koje daje etehničar.
- WiFi mreža je dostupna na pojasevima 2.4 i 5 Ghz. Dodatni pristup, predviđen je gostima koji nemaju AAI@Edu indentitet, i to putem mreže "Gosti" a za koju svaki gost mora dobiti podatke za pristup od e-školetehničara.
- Načelno je dozvoljeno priključivanje svih postojećih školskih uređaja, kao i privatnih prijenosnih uređaja (tableti, prijenosna računala i pametni telefoni). Dozvoljeno je spajanje na bežičnu mrežu i učenicima putem njihovih privatnih telefona ili tableta također sa njihovim AAI@Edu podacima. Korištenje učeničkih privatnih uređaja doozvoljeno je izvan nastave a na nastavi kad to izričito dozvoli predmetni nastavnik.
- Prilikom korištenja privatnih uređaja, korisnici su se također dužni držati pravila iz ovog pravilnika
- Priključivanje putem žične mreže za sada blokirano. Praktično svaki uređaj sa žičnim sučeljem se može slobodno priključiti na mrežu i koristiti lokalne resurse i internet. Štićeni resursi su međutim i dalje dostupni samo putem odgovarajućih autentifikacijskih metoda, korisničkih imena i zaporki.
- Spajanju gostujućih uređaja koji nisu dio školskog inventara potrebno je voditi računa tj korisnik mora dobiti usmeni pristanak za spajanje. Ukoliko se primjete učestale zlouporabe žične mreže ali i bežične mreže, etehničar može uvesti autentifikacijske metode i na žičnu mrežu, a počinitelje zlouporaba ili korištenja resursa suprotno ovompravidniku, može privremeno ili trajno onemogućiti

Nadzor mreže

- Cjelokupni promet mreže se nadzire putem odgovarajućih uređaja. Nadzor mreže i mrežnog prometa, kao i ispravnosti svih segmenata mreže vrši e-škole-tehničar te CARNET administratori. Nadzor je moguć daljinski preko web sučelja uz autorizirani pristup.
- Promet prema internetu i obrnuto je nadziran putem davaoca usluga spajanja a to je u našem slučaju riješeno ugovorom između CARNET-a i telekomunikacijske kuće koja osigurava širokopojasnu vezu s internetom.
- Mreža je osigurana od prometa neželjenog sadržaja u mjeri u kojoj je to tehnički moguće.
- Dodatne filtere može postavljati i sam e-škole-tehničar na lokalnom vatrozidu.
- Moguće je privremeno ili trajno blokirati spajanje i promet uređaja za koje utvrdi da generiraju neželjeni promet bilo radi infekcije malicioznim kodom ili radi zlouporabe od strane korisnika.
- E-tehničar je po zapažanju neželjenih i nedozvoljenih radnji ili nakon prijave od strane CARNET-a dužan locirati izvor, locirati korisnika i utvrditi razlog.
 - Ako je u pitanju zaraženo računalo, isto treba odspojiti od mreže i provesti postupak dijagnostike i čišćenja računala od malicioznog koda koje je najčešći uzrok takvih incidenata.
 - Ako je incident uzrokovao korisnik, e-tehničar je dužan korisnika upoznati s problemom kojeg je možda nesvjesno izazvao, objasniti mu zašto je do toga došlo i upozoriti ga na pravilan način upotrebe računala ili programskog alata, web sučelja ili web servisa. Tom prilikom e-tehničar mora biti jako oprezan odnosno nedvojbeno uvjeren u nedozvoljeni postupak korisnika prije nego povede bilo kakve mjere protiv nje ili njega. Ukoliko je nedvojbeno krivica na korisniku i ukoliko se unatoč upozorenja, incident ponavlja, korisnika treba privremeno ili trajno onemogućiti u korištenju resursa. Također korisnika treba prijaviti ravnatelju s opisom prekršaja koji je počinio te po mogućnosti priložiti dokaze.

SIGURNOST KORISNIKA

Pored svih tehničkih mjera navedenih u ovom pravilniku, neprestana edukacija korisnika je najvažniji faktor u općoj i sigurnoj upotrebi IKT-a. Korisnici su dužni i sami učiti iz dostupnih ili preporučenih izvora. Za opću IKT pismenost važnu ulogu imaju nastavnici informatike, e-tehničari, tečajevi, seminari, webinar, u organizaciji ministarstva obrazovanja i CARNET programa edukacije.

Pojava novih tehnologija važnih za školu ali i novih prijetnji sigurnosti treba što prije biti prenesena na korisnike škole. Nastavnici moraju biti dobro upoznati s pravilnim načinom uporabe IKT-a kao i opasnostima koje IKT nosi. To znanje treba neprestano biti prenošeno na učenike.

Prema postavkama, multikorisnička računala nemaju zaporke. Pristup kritičnim resursima je isključivo preko AAI@Edu identiteta i zaporki, i u pojedinim slučajevima pojačanim sustavom autentifikacije (tzv. dvostrukom provjerom) putem token uređaja ili putem pina ili putem pametnog telefona.

AAI@Edu je središnji sustav identifikacije, autentifikacije zaštite identiteta, osobnih podataka. Sustav se održava kako je propisano pravilnicima, uputama i preporukama CARNET-a.

- Svaki novi zaposlenik u školi dobiva AAI@Edu identitet i pri čemu se definira njegova uloga u sustavu, te temeljem toga korisnik automatski dobiva pristup određenim resursima. Najosnovnije, korisnik dobiva e-mail adresu ime.prezime@skole.hr i zaporku. Email adresa ujedno predstavlja njegovo korisničko ime.
- Promjenom uloga u sustavu sukladno se mijenjaju i korisnikova prava u sustavu. Prestankom radnog odnosa, korisniku se ukida AAI@Edu identitet ili se stavlja u mirovanje.
- Svaki novi učenik dobiva AAI@Edu identitet na početku školovanja, a briše ga se po završetku školovanja

PRIHVATLJIVO I ODGOVORNO KORIŠTENJE IKT-a

Ponašanje na internetu

Svaki pojedinac odgovara za svoje ponašanje na internetu. Osnova dobrog ponašanja je ta da se prema drugim korisnicima ponašamo pristojno, ne vrijeđamo, ne objavljujemo neprimjereni ili uvredljiv sadržaj bilo prema pojedincu, grupi, kulturi ili rasi.

Sve korisnike, a naročito učenike, potrebno je iznova podsjećati na oprez prilikom davanja osobnih podataka kao što su: ime i prezime, adresa, broj telefona, korisničko ime zaporka i druge podatke. Neophodno je redovito provoditi edukacije i upozoravati učenike na sve opasnosti interneta.

U komunikaciji putem društvenih mreža treba paziti da se ne povrijede tuđi osjećaji ili da se odaju tuđi podaci, ali treba paziti i na predatore, koji mame nevine korisnike i navode ih na davanje podataka.

Autorsko pravo

Korisnike, a naročito učenike treba poučavati o autorskim pravima i načinima korištenja tuđih radova. Nedozvoljeno je na primjer korištenje tuđih fotografija, slika tekstova, videa i drugih radova, bez eksplicitne dozvole autora. To je kršenje autorskih prava.

Autora treba kontaktirati i zatražiti dozvolu za korištenje njegovog rada s točnim opisom načina korištenja istog. Tek kad nam autor pismeno odobri smijemo koristiti njegov rad na način kako nam je autor odobrio. Čak i kad imamo odobrenje autora, ne smijemo njegov rad proglasiti svojim, ne smijemo ga mijenjati ako autor to nije dozvolio.

Ukoliko su javno dostupni radovi objavljeni pod tzv. Creative Common licencom (<https://creativecommons.org>), ili sličnom, treba proučiti gradaciju CC licence i koristiti rad sukladno nivou zaštite koju je autor primijenio. Potrebno se upoznati sa vrstama dozvola koje CC i slične licence definiraju, te je u svakom pojedinom slučaju potrebno poštovati nivo licence.

Na primjer CC licenca može biti dozvoljavati neograničenu upotrebu nekog rada u neprofitnoj primjeni. Može dozvoljavati čak i izmjene originalnog rada. Može zahtijevati eksplicitno

navođenje autora i poveznice do autorove web stranice ili do objavljenog rada. Varijacija ima puno. Najvažnije je znati da je korištenje tuđih radova u najvećem broju slučajeva povreda autorskih prava.

Također možemo, nekad je poželjno ili je čak i obavezno vlastite radove potpisati ili označiti CC licencom.

Iz svega navedenog, učenici se trebaju suzdržavati a nastavnici ih trebaju na to ne poticati, od preuzimanja tuđih radova, a za izradu nekih svojih projekata. Odnosno učenici moraju razvijati naviku poštovanja autorskih prava drugih autora, te shvaćati vlastita autorska prava za vlastite radove.

Dijeljenje datoteka

Razmjena datoteka preko mreže (e-mailom, ili preuzimanjem sa linkova, ili preko USB memorija, CD-ova i dugih medija) može biti vrlo opasna. Skriveni maliciozni kod u nekoj izvršnoj datoteci može napraviti veliku štetu na računalu, mreži, nanijeti nesagledive štete ustanovi ili tvrtki. Stoga, treba biti krajnje oprezan. Kao prvo izbjegavati otvaranje datoteka sa izvršnim nastavcima exe, com, sh, zip, rar, jar, čak i PDF. Te mnogim drugim.

Ne skidati programe sa interneta koji obećavaju popraviti ili ubrzati računalu, ne tražiti i ne preuzimati tzv crack aplikacije ili razbijene programe koje inače treba legalno kupiti. Naime, sve takve datoteke sadrže brojne neželjene i opasne programske kodove, čiji cilj je ugroziti sigurnost korisnika i njegovog računala, krađe podataka, krađe zaporki i mnogo drugih zlonamjernih radnji.

U školi se strogo zabranjuje preuzimanje i instalacija bilo kakvih datoteka, bez prethodne provjere sa etehničarem. Svaka se sumnjiva datoteka može višestruko ispitati prije nego se odluči otvoriti i upotrijebiti.

Internetsko nasilje - Nasilje preko interneta – cyberbullying

Nasilje preko interneta, u svijetu poznato kao cyberbullying, opći je pojam za svaku komunikacijsku aktivnost cyber tehnologijom koja se može smatrati štetnom kako za pojedinca, tako i za opće dobro. Tim oblikom nasilja među vršnjacima obuhvaćene su situacije kad je dijete ili tinejdžer izloženo napadu drugog djeteta, tinejdžera ili grupe djece, putem interneta ili mobilnog telefona.

Svako nasilje strogo će se sankcionirati

Korištenje mobilnih telefona u školi

- Korištenje mobilnih telefona u školi detaljnije je regulirano Kućnim redom škole
- Nije dozvoljena upotreba mobilnog telefona u školi za vrijeme nastave. Za vrijeme nastave učenici moraju svoje mobitele isključiti ili stišati (vibracija nije dozvoljena).
- Učitelj može zatražiti od učenika da pri ulasku u razred mobitel ostave na stolu ili mjestu koje je on odabrao.
- Za vrijeme pisanja pismenih provjera učenici su dužni pri ulasku predati mobitele.
- Svako korištenje mobitela u razredu za vrijeme nastave ili snimanje u razredu i hodnicima strogo je zabranjeno. U slučaju kršenja ovih uputa mobitel će se oduzeti od učenika i isti

će biti predan roditelju u tajništvu škole. Za potrebe nastave može se koristiti mobilni telefon (pametni telefon) ukoliko je učitelj najavio i dozvolio upotrebu.