

Osnovna škola Eugena Kumičića Slatina

Dobriše Cesarića 24

Slatina

**PRAVILNIK O SIGURNOJ I ODGOVORNOJ
UPOTREBI INFORMACIJSKO-KOMUNIKACIJSKE TEHNOLOGIJE
OSNOVNE ŠKOLE EUGENA KUMIČIĆA SLATINA**

Slatina, ožujak 2018.

Na temelju člana _____. Statuta škole Školski odbor na sjednici održanoj _____. donosi Pravilnik o sigurnoj i odgovornoj upotrebi informacijsko-komunikacijske tehnologije

I. UVOD

Članak 1.

Sukladno sve većom sustavnom uporabom IKT-a u školama, potrebno je voditi računa o prijetnjama informacijskom sadržaju i IKT infrastrukturi koje mogu rezultirati različitim oblicima štete informacijskom sustavu škole (npr. gubitak informacija, nemogućnost pristupa resursima i informacijskom sadržaju, uništenje opreme i sl.). Zbog toga je potrebno veliku pozornost potrebno posvetiti vidu sigurnog i odgovornog korištenja IKT-a, što je moguće postići definiranjem sigurnosne politike škole.

U školi je u siječnju 2106. godine postavljena infrastruktura CARNetove mreže.

Pravilnik vrijedi za sve korisnike IKT infrastrukture škole.

Učenici, učitelji i svi školski djelatnici se moraju pridržavati uputa koje im može dati administrator sustava (e-Škole tehničar).

Učenici i vanjski korisnici se moraju pridržavati uputa koje im može dati: učitelj i školski djelatnici ili administrator sustava (e-Škole tehničar).

U Osnovnoj školi Eugena Kumičića e-škole tehničarem imenovana je tvrtka V-Comp Slatina.

Pravilnik o sigurnoj i odgovornoj upotrebi informacijsko-komunikacijske tehnologije je dio sigurnosne politike škole. Oblikovan je uzimajući u obzir materijale dostupne na mrežnoj stranici <http://www.petzanet.hr> koji su nastali kao rezultat projekta usmjerenog ka sigurnosti djece na internetu, te dokumente Nacionalnog CERT-a koji se bave sigurnošću i privatnošću na internetu, dostupni na <http://www.cert.hr>.

Pravilnik je donesen sa svrhom:

- unaprjeđenja sigurnosti školske informatičke opreme i mreže.
- jasno i nedvosmisleno odrediti načine prihvatljivog i dopuštenog korištenja IKT resursa škole
- zaštite informacijskog sadržaja i opreme
- zaštite korisnika od različitih vrsta internetskog zlostavljanja
- promoviranja sustava i usluga koji su najprikladniji za djecu
- poticanja aktivnog sudjelovanja djece u radu s IKT-om promovirajući sigurno, odgovorno i učinkovito korištenje digitalnih tehnologija u mrežnoj zajednici pravilne raspodjele zadatke i odgovornosti nadležnih osoba
- propisivanja sankcija u slučaju kršenja odredbi Pravilnika

II. OSNOVNE SIGURNOSNE ODREDBE

Članak 2.

Materijalni i nematerijalni resursi su:

- Korisnici IKT infrastrukture su učenici, učitelji, ostali djelatnici i povremeni korisnici (gosti).
- Kompletna računalna mreža izgrađena u sklopu pilot projekta e-Škole i računalna oprema, stara računalna mreža i računalna oprema smatraju se IKT infrastrukturom.
- U školi postoje interne, javne, povjerljive informacije.
- Aplikacije koje škola koristi: e-Dnevnik, e-Matica, HUSO admin, Obračun plaća s evidencijom kadrova (Funkcija 13), Meraki (središnji sustav za upravljanje računalnom mrežom), Office 2016 skup programa, Windows operativni sustav

Školska oprema se mora čuvati i pažljivo koristiti.

Tuđi i osobni podaci škole mogu se koristiti isključivo samo uz prethodno odobrenje ravnatelja škole.

S obzirom na dostupnost financija sigurnosne mjere zaštite podataka su na prosječno zadovoljavajućoj razini. Trenutno sva računala koja su na Windows operativnim sustavima posjeduju vatrozid i antivirusni program (odnosi se na Windows 7 i starije operativne sustave (Windows xp). Noviji operativni sustavi, poput Windows 8.1 i 10, posjeduju Windows Defender Security Center. Učenici, učitelji, ostali djelatnici i gosti koji se spajaju na računalnu mrežu sa svojim privatnim pametnim telefonima i ostalim uređajima čiji su sustavi android, ios, windows operativnim sustavima imaju zaštitu vatrozida na razini prometa prema internetu, ali ne unutar škole, te nemaju nikakvu antivirusnu zaštitu.

Većina mjera zaštite su implementirana kod davatelja internetski usluga (ISP-a - CARNet).

Njihovi serveri blokiraju sadržaje i stanice sumnjivog karaktera. U našem mrežnom sustavu je blokiran pristup P2P (peer to peer) mrežnom servisu za razmjenu podataka, te web stranicama koji podržavaju P2P razmjenu podataka.

Svi zaposlenici naše škole posjeduju AAI@EduHr korisnički račun pa su tako dužni koristiti email koji su dobili iz AAI@EduHr sustava (netko.netko@skole.hr) u službenoj komunikaciji s nadležnim tijelima i drugim institucijama iz sustava znanosti i obrazovanja. Također, preporuča se korištenje istog emaila za komunikaciju među djelatnicima unutra škole za poslove vezane uz školu.

Učiteljima i drugim djelatnicima je strogo zabranjeno davati učenicima i drugim korisnicima vlastite zaporke i druge digitalne identitete (token, tajne poveznice i sl.).

Svi djelatnici škole moraju potpisati izjavu o tajnosti podataka te se moraju pridržavati etičkih načela pri korištenju IKT-a.

Svako nepridržavanje pravila od strane zaposlenika i svako ponašanje koje nije u skladu s Pravilnikom prijavljuje se ravnatelju škole, a sankcionirati će se temeljem važećih općih akata škole.

Ozbiljniji incidenti prijavljuju se CARNetovom CERT-u, preko obrasca na mrežnoj stranici www.cert.hr.

III. ŠKOLSKA IKT OPREMA I ODRŽAVANJE

Članak 3.

Računalna mreža je skupina od 2 ili više međusobno povezanih računala. Računala u školi su povezana bežično i žičano. Računalna mreža se sastoji od novog dijela koje je izgrađen u sklopu e-Škole projekta te starog dijela mreže. U sklopu e-Škole projekta od osnivača škole (Virovitičko-podravska županija) imenovan je e-tehničar koji je zadužen i plaćen za održavanje navedene mrežne infrastrukture.

Računalni otpad odvozi ovlaštena tvrtka Flora Vtc d.o.o. Virovitica.

Računala u matičnoj školi se bežično spajaju na 28 bežičnih pristupnih točaka. Pristupne točke su smještene u svakoj učionici te u najvažnijim prostorima škole (zbornica, hol, konferencijska dvorana, sportske dvorane).

Određena računala u školi su spojena žičanim načinom spajanja na mrežu. Uz minimalne troškove UTP kabel se može dovesti u bilo koju prostoriju ako se pojavi takva potreba.

Računala koja su spojena na taj način spojena su na također na novu mrežnu infrastrukturu.

Računala koja su spojena žičano su sva računala u informatičkoj učionici (17 računala), računala u uredima (tajništvo, računovodstvo, zbornica, pedagog, psiholog, zbornica).

Sveukupno 23 računalo je spojeno na računalnu mrežu žičanim putem. Računalna mreža je konfigurirana tako da nema potrebe da se računala/korisnici autentificiraju kada se spajaju u žičanu računalnu mrežu.

Računala u područnim školama bežično se spajaju na 1 bežičnu pristupnu točku u svakoj područnoj školi, dok se žičano spajaju preko dvostruke mrežne utičnice u svakoj učionici i zbornici..

Većina računala u školi posjeduje operativni sustav Windows s instaliranim Office alatima. Postavke na računalima su podešene na općenite te je na svim računalima postavljeno da kod prijave u operativni sustav nema zaporke. Na zahtjev pojedinih djelatnika koji imaju osjetljive podatke na računalima postavljena je lozinka za pristup računalu. Također je uključena opcija da lozinka nikada ne ističe (Password never expires). Kod svih računala je podešeno ažuriranje operativnog sustava i popratnih office alata na automatski. Analiza prometa računalne mreže pokazuje da najviše prometa koja računala ostvaruju preko interneta odlazi na ažuriranje navedenog. Operativni sustavi Windows 10 imaju u sebi obrambeni sustav (Windows Defender Security Center) te također i vatrozid koji posjeduju i stariji operativni sustavi do Windows XP-a. Antivirusni programi ako se koriste, koriste se na starijim operativnim sustavima i to besplatne inačice antivirusnih programa (AVG AntiVirus Free, Avast Free Antivirus). Od filtriranja sadržaja trenutno se filtriraju web stranice koje promoviraju i sadrže P2P (peer to peer) datoteke. Računalna mreža u potpunosti blokira promet P2P.

Trenutno u školi nema potrebe samostalnog nadziranja licenciranih programa jer svi programi koji se koriste (Windows XP, Vista, 7, 8, 8.1, 10, Office 2007, 2010, 2013, 2016) su licencirani

od strane Ministarstva znanosti i obrazovanja i tvrtke Microsoft. Ministarstvo znanosti i obrazovanja je izradilo web portal Centar za preuzimanje Microsoft proizvoda. Pristup portalu imaju svi odgovorni za održavanje i instalaciju računalnih programa u školama (administratori sustava, e-tehničari). U sustav se prijavljuje AAI@edu korisničkim računom gdje se mogu preuzeti svi navedeni operativni sustavi i office alati s pripadajućim ključevima za aktivaciju.

Učenici smiju instalirati dodatne računalne programe u informatičkoj učionici (igrice ili nekakav drugi program) na lokalnu C particiju. Računala u informatičkoj učionici su postavljena tako da je C lokalna particija "zamrznuta" (program Reboot Restore RX) što znači da ako učenici nešto postave, instaliraju, obrišu u operativnom sustavu nakon ponovnog pokretanja računala s isto se vraća u prvobitno stanje.

Na ostala računala u školi učenici ne smiju ništa instalirati bez odobrenja administratora ili učitelja. Ako se pojavi potreba za instaliranje dodatnog programa učenik se mora obavezno javiti administratoru ili učitelju. Učiteljima je dopušteno samostalno instalirati programe potrebne za nastavu koje su dobili od izdavača odabranih udžbenika ili neki drugi program koji omogućava korištenje IKT u nastavi. Učitelji su upoznati s programima pogodnim za korištenje IKT u nastavi kroz radionice projekta eŠkole, te kroz radionice koje škola kontinuirano provodi u sklopu učiteljskih i stručnih vijeća.

Svako nepridržavanje ovih pravila ima negativan utjecaj po Školu i može rezultirati disciplinskim mjerama prema djelatnicima Škole ili pedagoškim mjerama prema učenicima sukladno Pravilniku o kriterijima za izricanje pedagoških mjera.

IV. REGULIRANJE PRISTUPA IKT OPREMI

Članak 4.

Računalnoj mreži mogu pristupiti učenici, učitelji, ostali djelatnici škole te vanjski partneri i posjetitelji.

Pristup bežičnoj računalnoj mreži je zaštićen na nekoliko načina. Pristup ovisi o tome tko se želi spojiti na mrežu i s kojim razlogom.

U bežičnim pristupnim točkama su postavljene tri naziva za pristup bežičnoj mreži (SSID):

- eduroam,
- eSkole,
- guest,
- public (skrivena mreža).

Na eduroam mrežu se spajaju nastavnici i učenici sa svojim privatnim ili školskim uređajima gdje se autentificiraju svojim korisničkim podacima iz AAI@EduHr sustava (802.1x with custom RADIUS enkripcija). Na taj način se može identificirati i pratiti njihov promet u računalnoj mreži.

eSkole mreža se koristi za spajanje uređaja u STEM učionicama gdje se učenici i nastavnici (samo u slučaju da koriste isti uređaj) spajaju preko Captive portala koji se aktivira prilikom procesa spajanja (WPA2-PSK password-protected with custom RADIUS enkripcija).

Guest mreža se koristi za spajanje vanjskih partnera i posjetitelja (Open-passwordprotected with Meraki RADIUS enkripcija). Partnerima i posjetiteljima koji imaju AAI@edu račun je omogućen pristup na eduroam mrežu uz ograničenje brzine pristupa. Ostalim partnerima i posjetiteljima se može na zahtjev omogućiti pristup bežičnoj mreži. Bežična mreža guest je otvorenog tipa, a za autentikaciju se koristi tzv. captive portal. Kako bi im se omogućio pristup, e-Škole tehničar u Meraki dashboardu mora kreirati korisničko ime za svakog korisnika kojem škola odobri pristup mreži.

Public mreža namijenjena je javnim računalima u knjižnici, porti, xbox koja nisu obuhvaćena žičanom računalnom mrežom, te se spajaju bežičnom računalnom mrežom. Public bežična mreža potpuno je odvojena od ostalih bežičnih mreža u školi i računala koja se spajaju na nju su ograničena samo na pristup internetu malom brzinom koristeći više razina zaštite kako bi se osiguralo da nitko s javnih računala „ne vidi“ niti jedan uređaj u računalnoj mreži (računalo, pisač,...).

Učitelji iz STEM područja su dobili hibridno računalo Fujitsu, ravnateljica, stručne suradnice, učitelji na područnim školama su dobili Fujitsu prijenosno računalo, a ostali nastavnici Samsung tablet.

STEM učionice (učionice matematike i kemije) su opremljene Samsung tabletima koji učenici mogu koristiti samo uz odobrenje nastavnika. Učitelji imaju pristup računalu i mrežnom pisaču koji su smješteni u zbornici.

Ostali učitelji i stručni suradnici mogu koristiti informatičku učionicu uz prethodni dogovor s učiteljima informatike kako bi se osiguralo neometano izvođenje nastave informatike te kako bi se odgovarajuće pripremila informatička učionica za potrebe predavanja/radionice.

Učenici smiju koristiti računala samo uz dopuštenje učitelja.

Na nastavi informatike učenici ako su prethodno dobili odobrenje od učitelja za uključivanje računala smiju pod odmorom koristiti računalo za svoje potrebe. Eventualno na kraju drugog sata (nastava informatike se održava dva sata zaredom) ako su učenici uspješno prošli sve etape nastavnog procesa tada smiju koristiti računalo uz odobrenje nastavnika (za pristup internetskim sadržajima i za zabavu).

U STEM učionicama učenici također smiju koristiti računalnu opremu samo uz odobrenje učitelja. Pristup aplikacijama i internetskim sadržajima određuje isključivo učitelj.

Učenici uz odobrenje učitelja smiju koristiti svoje privatne uređaje za spajanje, ali samo uz izričito dopuštenje učitelja.

Svi učitelji koji koriste informatičku učionicu moraju se držati navedenog:

- učionica mora ostati na kraju onako kako je i zatečena,
- računala se obavezno moraju ugasiti nakon uporabe,
- u slučaju da jedno od računala ne radi – kontaktirati učitelje informatike,
- radna mjesta moraju ostati čista,
- radno mjesto mora ostati uredno – namještena tipkovnica, miš, monitor, stolica na svojem mjestu,
- prozore obavezno zatvoriti,
- učionicu zaključati.

Učitelj informatike je odgovoran za informatičku učionicu dok u njoj izvodi nastavu. Ostali učitelji i stručni suradnici odgovorni su za učionicu informatike dok u njoj izvode nastavu/radionice.

U slučaju da bude bilo potrebe za korištenjem korisničke zaporke u nastavku slijedi smjernica za izradu; ne smije biti kraća od šest (6) znakova, da ima kombinaciju velikih/malih slova, da mora imati minimalno jedan broj i jedan poseban znak.

Odlukom Ministarstva znanosti i obrazovanja prema kojoj se sve osnovne i srednje škole spojene na CARNetovu mrežu automatski su uključene u sustav filtriranja nepoćudnih sadržaja. Dodatno je uključeno u našem mrežnom sustavu blokiranje pristupa P2P (peer to peer) mrežnom servisu za razmjenu podataka te web stranicama koji podržavaju P2P razmjenu podataka.

V. SIGURNOST KORISNIKA

Članak 5.

U školama je potreba neprekidna edukacija učenika, učitelja i cijelog školskog kolektiva kako bi se mogao održati korak u korištenju IKT-a, kao i s nadolazećim prijetnjama u računalnoj sigurnosti.

Sva računala i programi koji zahtijevaju prijavu moraju posebno voditi računa da kod prijave ne otkriju svoje podatke za prijavu. Isto tako učitelji kada odlaze iz učionice, a ostavljaju računalo uključeno obavezno se moraju odjaviti iz svih sustava u koje su se prijavili. Ukoliko učenici koriste računala u STEM učionicama obavezno nakon završetka rada moraju se odjaviti iz sustava u koje su se prijavili.

Učenici, učitelji i ostali djelatnici moraju posebno voditi računa o svojem digitalnom identitetu koji su dobili iz sustava AAI@edu. Svoje podatke moraju čuvati.

Zasada je dopušteno u potpunosti preuzimanje datoteka na lokalna računala te pokretanje izvršnih datoteka. Ako vrijeme pokaže da se na taj način računala inficiraju zlonamjernim programima, e-tehničar će uvesti restrikciju na takvu vrstu interakcije.

Svi učenici, učitelji te ostalo osoblje posjeduje Elektronički identitet u sustavu [AAI@Edu.hr](https://www.aai.edu.hr). U školi se često izvodi revizija korisničkih računa. Svi učenici dobivaju elektronički identitet ispisan u analognom obliku te ima se daje na čuvanje i korištenje. U slučaju da izgube svoj korisnički račun, učenik ili roditelj dolazi u tajništvo škole gdje tajnik škole ispisuje korisnički račun s novom lozinkom. U slučaju da učenik seli iz naše škole u neku drugu školu, njegov elektronički identitet se privremeno briše. U slučaju da učenik iz neke škole dolazi u našu školu njegov elektronički identitet se prenosi u našu školu. Isto vrijedi i za učitelje i ostalo osoblje.

Učenicima prestaju prava nad elektroničkim identitetom kada završe sa svojim školovanjem.

Učiteljima i ostalom osoblju prestaju prava kada završe sa svojim radnim vijekom tj. odlaskom u mirovinu ili prestankom rada u školskom sustavu.

Učenici su upoznati s informacijama o sustavu odnosno da je sustav podešen tako da filtrira nepoćudan sadržaj, to im se posebno naglašava te se o istome educiraju i upućuju na nastavi informatike. Učenici su stalno pod nadzorom te im je u potpunosti onemogućeno zaobilaženje sigurnosnih postavki računalne opreme.

U školi postoji nadzor mrežnog prometa kroz Meraki Cloud System od strane e-tehničara škole.

VI. PRIHVATLJIVO I ODGOVORNO KORIŠTENJE INFORMACIJSKO-KOMUNIKACIJSKE TEHNOLOGIJE (PONAŠANJE NA INTERNETU)

Članak 6.

Svaki pojedinac je odgovoran za svoje ponašanje u virtualnom svijetu te se prema drugim korisnicima mora ponašati pristojno, ne vrijeđati ih niti objavljivati neprimjerene sadržaje. U virtualnom svijetu svaki pojedinac bi se trebao ponašati kao i u stvarnom svijetu.

Za svakog korisnika koji se susreće s internetom nužno je prvo upoznati ga s osnovnim pravilima ponašanja u takvoj komunikaciji i takvom okruženju. To se još naziva i 'internetskim bontonom', a vrlo čest naziv je i 'Netiquette'. 'Netiquette' je ustaljen popis pravila lijepog ponašanja u internetskoj komunikaciji i preveden je na mnoštvo jezika. Hrvatske stranice dostupne su na <http://hr-netiquette.org>. 'Netiquette' propisuju smjernice i pravila ponašanja u tri (3) kategorije: elektronička pošta, popis e-adresa i forumi.

Škola je ovaj skup pravila učinila dostupnim svojim učenicima, o tome ih podučava, te primjenjuje vlastitu politiku u skladu s tim pravilima.

Ovaj skup pravila je izvješten u informatičkoj učionici te je objavljen na mrežnoj stranici škole.

a) Elektronička pošta:

- Ukoliko ne koristite postupke enkripcije (hardware ili software), morate znati da elektronička pošta na Internetu nije sigurna. Nemojte nikada staviti u e-mail ono što ne biste stavili na dopisnicu.
- Poštujte vlasnička prava nad materijalima koje reproducirate. Skoro sve zemlje imaju zakone o vlasničkim pravima.
- Ukoliko prosljeđujete poruku koju ste primili, ne mijenjajte sadržaj. Ako je to bila osobna poruka upućena vama i vi je preusmjeravate grupi, zatražite dopuštenje. Možete ju kratiti i citirati samo dijelove od značaja, ali naznačite njezinog autora.
- Nikada ne šaljite "lance sreće" elektroničkom poštom. "Lanci sreće" su zabranjeni na Internetu. Pristup mreži (ili servisu ili forumu) vam može biti uskraćen.
- Olakšajte stvari primatelju. Mnogi programi za e-mail izbrišu podatke iz zaglavlja koji sadrže adresu za odgovor. Da biste bili sigurni da ljudi znaju tko ste, uključite liniju ili dvije na kraju poruke s podacima za kontakt. Možete napraviti datoteku s kontaktnim podacima i uključivati ga na kraj vaših poruka. Neki programi to rade automatski. U Internet žargonu to je poznato kao .sig ili signature datoteka. Vaša .sig datoteka će nadomjestiti vašu posjetnicu, a možete ih imati nekoliko za različite prigode.
- Ukoliko uključujete signature datoteku, pazite da bude kratka. Preporučljiva duljina bila bi ne više od četiri linije. Imajte na umu da mnogi ljudi plaćaju pristup Internetu po količini podataka i što je vaša poruka dulja, oni više plaćaju.

- Budite oprezni prilikom slanja elektroničke pošte. Postoje adrese koje predstavljaju grupu ljudi, a izgledaju kao da se radi o jednoj osobi. Znajte kome šaljete e-mail.
- Imajte na umu da je primatelj ljudsko biće, čija se kultura, jezik i smisao za humor mogu razlikovati od vaših. Problema može biti i s oblikom zapisa datuma, s mjernim jedinicama i idiomima. Budite osobito oprezni sa sarkazmom.
- Ne koristite isključivo velika slova. VELIKA SLOVA IZGLEDAJU KAO DA VIČETE.
- Koristite smileye da naznačite ton, ali koristite ih s mjerom. :-) je primjer smileya (nakrivite glavu). Nemojte misliti da će time primatelj nužno biti zadovoljan sadržajem poruke ili da ćete time poništiti uvredljivu poruku.
- Cijenu slanja elektroničke pošte plaćaju, u prosjeku, podjednako pošiljatelj i primatelj (ili njihove organizacije). To je različito od drugih medija kao što su poštanske pošiljke, telefon, TV ili radio. Primatelj elektroničke pošte može imati troškove kao što su širina pojasa (širina internet veze, bandwidth), diskovni prostor ili korištenje procesora. To je osnovni ekonomski razlog zašto nezatraženo e-mail oglašavanje nije dobrodošlo (i u raznim kontekstima je zabranjeno).
- Ne šaljite velike količine podataka ljudima koji ih nisu zatražili.

b) Mailing liste, news grupe (usenet)

Sva pravila za elektroničku poštu vrijede i ovdje.

- Čitajte mailing liste i news grupe mjesec ili dva prije nego što na njih nešto pošaljete.
- Ovo će vam pomoći razumjeti pravila ponašanja grupe.
- Ne okrivljajte sistem administratora zbog ponašanja korisnika sistema.
- Pretpostavite da pojedinci govore u svoje osobno ime i da ono što napišu ne predstavlja njihovu organizaciju (osim ako nije eksplicitno navedeno).
- Imajte na umu da i elektronička pošta i news troše resurse sistema. Obratite pozornost na sva pravila koja vaša organizacija može imati o korištenju ovih resursa.
- Poruke i članci trebaju biti kratki i u vezi s onim o čemu se raspravlja. Ne skrećite s teme, suvislo se izražavajte i ne šaljite poruke samo zato da bi ukazali na tuđe greške u tipkanju ili pravopisu. Ovakvo ponašanje će vas, više od bilo čega, označiti kao nezrelog početnika.
- Krivo predstavljanje nije dopušteno.
- Oglašavanje je dopušteno na nekim listama i grupama, a osuđivano na drugima! Ovo je još jedan primjer zašto treba upoznati auditorij prije slanja poruke. Nezatražene reklamne poruke koje se ne tiču teme rasprave će sigurno uzrokovati da dobijete mnogo ljutih odgovora.

- Pročitajte sve članke u slijedu (thread) prije nego šaljete odgovor. Ne šaljite "Ja također" poruke čiji sadržaj je ograničen na slaganje s prethodnom porukom. Sadržaj poruke bi trebao proširivati onu na koju se nadovezuje.
- Pošaljite odgovor elektroničkom poštom ako se tiče samo jedne osobe. Newsi se globalno distribuiraju i cijeli svijet vjerojatno **nije** zainteresiran za osobne odgovore.
- Nemojte, međutim, oklijevati da pošaljete nešto od interesa za sve sudionike u raspravi.
- Ako mislite da je članak od interesa za više grupa, budite sigurni da ga crosspostate, a ne da ga šaljete posebno u svaku grupu. Općenito, ne više od pet - šest grupa će imati interese dovoljno slične da bi se to činilo.
- Razmislite o korištenju priručnika, knjiga, help datoteka i sl. prije nego što postavite pitanje. Postavljanje na newsima pitanja za koje postoje odgovori na drugim mjestima imat će za posljedicu mrzovoljne "RTFM" odgovore (read the fine manual - iako i vulgarno značenje za "F" riječ postoji).
- Iako postoje news grupe u kojima je oglašavanje dopušteno, općenito se smatra kriminalnim činom oglašavati proizvode koji se ne tiču same rasprave. Ako pošaljete oglasnu poruku na mnogo grupa, vjerojatno ćete izgubiti pravo na pristup Internetu!
- Predstavljanje tuđim imenom u news člancima nije dopušteno. Od toga se možete zaštititi korištenjem softwera koji generira "otisak prsta" kao što je PGP.

c) Forumi

- Prije svega
 - Ako postoje pravila foruma, obavezno ih pročitajte ih pridržavajte ih se.
 - Ako postoji FAQ lista (često postavljana pitanja), obavezno je pročitajte. Možda ćete upravo tamo naći informaciju koju ste tražili.
- Nazivanje i otvaranje tema
 - Dobro pregledajte forum i budite sigurni da započnete raspravu u pravom dijelu foruma.
 - Prije nego li započnete temu, pretražite forum i potražite sličnu temu. Možda već postoji rasprava poput one koju namjeravate započeti.
 - Naslov vaše teme mora bit deskriptivan, odnosno, iz naslova mora biti jasno o kojoj se temi radi.
 - Naslov teme mora biti kratak i jasan.
- Pisanje poruka
 - Razmislite prije nego li napišete **bilo što**. Morate imati valjan razlog za pisanje poruke, a ona mora biti *smisljena*.

- Pažljivo sročite svoju poruku. Nastojte da bude što jasnija i jednoznačna. Izbjegavajte nesporazume, koliko je to moguće.
- Pišite u prijateljskom tonu.
- Prije nego li pošaljete poruku, provjerite jeste li sve napisali kako se htjeli.
- Kada nastavljate raspravu, pročitajte sve prijašnje poruke kako bi bili sigurni da nećete dodati informaciju koja već postoji.
- Ako u vrlo staru temu dodajete novu poruku, budite sigurni da je ona vrijedna toga.
- Uvijek nastojte poštivati temu.
- Ne koristite isključivo velika slova. VELIKA SLOVA IZGLEDAJU KAO DA VIČETE
- Citiranje
 - Kod odgovora (reply), citirajte poruku na koju odgovarate.
 - Ukoliko je poruka na koju odgovarate dugačka, citirajte samo bitne dijelove.
- Privatni razgovori
 - Privatnih razgovori na javnom dijelu foruma nisu poželjni. Za njih, koristite privatne poruke, ukoliko postoje, ili e-mail.
- Potpisi
 - Nastojte da vaši potpisi budu što kraći i neupadljivi.
 - Nastojte ne stavljati slike u potpise.

Učenike se poučava kroz nastavu informatike i satova razrednika da ne otkrivaju osobne podatke, svoju adresu, ime škole, telefonske brojeve i slično preko interneta (na servisima popu Facebooka, Twitera, chat sobe...).

Pravila sigurnog ponašanja:

- Osobne informacije na internetu se nikad ne smiju odavati.
- Zaporka je tajna i nikad se ne smije nikome reći.
- Ne odgovarajte na zlonamjerne ili prijeteće poruke! Prijavite ih!
- Treba pomoći prijateljima koji su zlostavljani preko interneta tako da se to ne prikriva i da se odmah obavijeste odrasli.
- Provjeriti je li Facebook profil skriven za osobe koji nam nisu 'prijatelji'. Treba biti kritičan prema ljudima koji se primaju za 'prijatelje'.
- Potrebno je biti oprezan s izborom fotografija koje se objavljuju na Facebooku.
- Treba provjeriti postoji li neka mrežna stranica o nama te koje informacije sadrži (*treba upisati svoje ime i prezime u Google*).

VII. AUTORSKO PRAVO

Članak 7.

Autorska prava na online dokumentima najčešće se definiraju s tzv. Creative Commons (CC) licencama (više na : <https://creativecommons.org/licenses/?lang=hr>). Creative Commons licence jesu skup autorsko-pravnih licenci pravovaljanih u čitavom svijetu. Svaka od licenci pomaže autorima da zadrže svoja autorska prava, a drugima dopuste da umnožavaju, distribuiraju i na neke druge načine koriste njihova djela, barem u nekomercijalne svrhe. Svaka Creative Commons licenca osigurava davateljima licence i da ih se prizna i označi kao autore djela.

Učitelji, učenici i ostali djelatnici se potiču da potpisuju materijale koji su sami izradili koristeći neku licencu te da poštuju tuđe radove. Nipošto ne smiju tuđe radove predstavljati kao svoje, preuzimati zasluge za tuđe radove, niti je dozvoljeno primati tuđe radove s interneta.

Korištenje tuđih radova s interneta mora biti citirano, obavezno navodeći autora korištenih materijala te izvor informacije (poveznica i datum preuzimanja).

Računalni programi su također zaštićeni zakonom kao i jezična djela. Najčešće su zaštićeni samo izvorni programi, no ne i ideje na kojima se oni zasnivaju. U to su uključeni naravno i on-line programi odnosno web aplikacije.

Kod mrežnih mjesta moguće je posebno zaštititi samo objavljeni sadržaj, a moguće je zaštititi i elemente koji se odnose na samo mrežno mjesto i djelo su dizajnera i/ili tvrtke/osobe koja je izradila samo mrežno mjesto.

VIII. DIJELJENJE DATOTEKA

Članak 8.

Prednost digitalnog sadržaja je da se ne uništava ili mu se ne umanjuje kvaliteta s brojem kopiranja. Ipak, baš zbog tog vida potrebno je biti vrlo oprezan s korištenjem digitalnih materijala, a još više s njihovim dijeljenjem. Naime, dijeljenje datoteka, samo po sebi, nije nelegalno. U slučaju da je datoteka proizvod pojedinca, pojedinac je može bez problema podijeliti s drugima na različite načine. Pritom je, dakako, uputno zaštititi djelo nekom vrstom prikladne licence.

Primjer nelegalnog dijeljenja datoteke jeste kopiranje ili preuzimanje autorski zaštićenog materijala poput e-knjige, glazbe ili pak videosadržaja. Mnogi online servisi danas omogućuju preuzimanje glazbenih albuma, pjesama, videosadržaja ili pak e-knjiga na nelegalan način. Primjer su klijenti (npr. Torrent) koji omogućuju dijeljenje sadržaja između računala pa se tako dijele najčešće nelegalno nabavljeni videosadržaji te glazbeni sadržaji, ključevi za korištenje različitih aplikacija i drugi digitalni sadržaji koji su zaštićeni autorskim pravima, gdje je izričito zabranjeno daljnje distribuiranje i umnožavanje bez dozvole autora ili bez plaćanja naknade. Postoje i različiti oblici mrežnog servisa koji omogućuju registraciju korisnika za vrlo nisku mjesečnu pretplatu te nude preuzimanje gotovo neograničene količine digitalnog sadržaja koji je zaštićen autorskim pravom, no to je također nelegalno.

U školi se izričito zabranjuje nelegalno kopiranje ili preuzimanje autorski zaštićenog materijala.

Računalna mreža je postavljena tako da u potpunosti onemogućava P2P (peer to peer) protokole i filtrira mrežne stranice koje sadrže P2P datoteke. U potpunosti je onemogućeno korištenje popularno zvanih torrenata. Torrent klijenti će se moći instalirati i pokrenuti ali neće moći ostvariti nikakav mrežni promet.

Obaveze ustanove su:

- Učenike i učitelje podučiti o autorskom pravu i intelektualnom vlasništvu.
- Učenike i učitelje podučiti i usmjeriti na korištenje licenci za zaštitu autorskog prava i intelektualnog vlasništva. Mogu se koristiti materijali s <https://creativecommons.org/licenses/?lang=hr>
- Učenike i učitelje informirati o mogućim načinima nelegalnog dijeljenja datoteka i servisima koji to omogućuju poput *Torrent* servisa, mrežnog mjesta koja zahtijevaju registraciju i plaćanje vrlo niske članarine za neograničeno preuzimanje digitalnog sadržaja i sl.
- Učenike i učitelje informirati o mogućim posljedicama nelegalnog korištenja, dijeljenja i umnažanja autorski zaštićenih materijala.

IX. INTERNETSKO NASILJE

Članak 9.

Internetsko nasilje se općenito može definirati kao namjerno i opetovano nanošenje štete korištenjem računala, mobitela i drugih elektroničkih uređaja. 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.

Postoje različiti oblici internetskog zlostavljanja:

- nastavljanja slanja e-pošte usprkos tome što netko više ne želi komunicirati s pošiljateljem
- cyberbullying
- nasilje mobitelom
- nasilje na chatu
- nasilje na forumu
- nasilje na blogu
- nasilje na web servisima (društvene mreže)
- svi ostali oblici nasilja preko internet
- otkrivanje osobnih podataka žrtve na mrežnim stranicama ili forumima
- lažno predstavljanje žrtve na internetu
- slanje prijetećih poruka žrtvi koristeći različite internetske servise (poput Facebooka, Skypea, e-maila i drugih servisa za komunikaciju)
- postavljanje internetske ankete o žrtvi
- slanje virusa na e-mail ili mobitel
- slanje uznemirujućih fotografija putem e-maila, mms-a ili drugih komunikacijskih alata.

Nasilje u školama je postao sve veći problem tijekom nekoliko posljednjih godina, a budući da sve više djece koristi internet i mobilne telefone za komuniciranje, internetsko nasilje 'cyberbullying' je postalo velik problem. U nekim zemljama ovom se problemu pristupa u suradnji s udrugama ili drugim javnim tijelima koja djeluju u školama.

Iako se velika većina incidenata može riješiti neformalnim putem (zvanjem roditelja, slanja djece savjetniku i sl.), postoje i situacije kad se zahtijeva službena reakcija škole. To se događa u slučajevima koji uključuju ozbiljne prijetnje prema drugim učenicima, a rezultiraju time da žrtva više ne želi ići u školu ili pak ako se nasilje nastavi iako su već korištena druga neformalna sredstva. U takvim težim oblicima zlostavljanja potrebno je izreći neku od disciplinskih mjera škole.

Svi oblici nasilničkog ponašanja u školi su nedopušteni i disciplinski će odgovarati svi oni za koje se utvrdi da provode takve aktivnosti.

Potrebno je istaknuti da su svi oblici nasilničkog ponašanja nedopušteni i da će disciplinski odgovarati svi oni za koje se utvrdi da provode takve aktivnosti.

Edukacija o neprihvatljivom ponašanju provode se kroz predmete koji koriste tehnologiju, Sat razrednika, radionice koje provodi škola samostalno ili u sklopu većih inicijativa, te su pravila o prihvatljivom ponašanju i korištenju tehnologije vidljiva i u prostorijama škole.

Stručna služba škole provodit će savjetodavni rad s učenicima koji prolaze ili uzrokuju male oblike uznemiravanja, a kroz strategiju će se provesti i preventivne mjere suzbijanja nasilja.

Škola se obvezuje da će:

- Podučiti učenike i učitelje o mogućim oblicima internetskog nasilja.
- Učenike i učitelje podučiti o tome kako prepoznati internetsko nasilje.
- Jasno istaknuti prihvatljiva pravila ponašanja te učenike i učitelje podučiti kroz predmete koji koriste tehnologiju.
- Izraditi strategiju odgovora na internetsko nasilje, i to na blaži i teži oblik.
- Razviti nultu stopu tolerancije na internetsko nasilje.
- Obilježavati Dane sigurnog korištenja interneta i suzbijanja nasilja kroz kreativne radove (npr. natječaj za najbolji videouradak, likovni ili literarni uradak na temu internetskog nasilja kako se potaknula svijest o temi među učenicima).

Prijedlozi strateških ciljeva OŠ Eugena Kumičića Slatina u području sigurnosti poslovanja:

CILJ 1.	Unaprjeđenje sigurnosti učenika na internetu
Mjera 1.1.	Unaprjeđenje suradnje s roditeljima
Cilj i opis mjere	<p>Cilj je u sljedeće četiri školske unaprijediti suradnju s roditeljima kroz povećano sudjelovanje roditelja u školskim aktivnostima u području IKT tehnologije. Kako bi škola postala uspješna organizacija, potrebno je da bude aktivni nositelj poticanja zajedništva i suradnje na relaciji učenik-nastavnik- roditelj.</p> <p>Povećana uključenost roditelja utjecat će na povećanu motivaciju učenika, postizanje boljeg uspjeha u školi, stvaranje bolje komunikacije između škole i roditelja, poboljšat će roditeljske kompetencije, nastavnicima omogućiti bolje poznavanje učenika, povećavanje kvalitete rada škole i povećanje ugleda škole u lokalnoj zajednici.</p> <p>Roditelji će biti aktivni suradnici ustanove kroz sudjelovanje na sastancima, individualnim razgovorima, razrednim projektima, školskim projektima, edukacijama za roditelje o sigurnosti na internetu, korištenju e-dnevnika i sl., izvannastavnim aktivnostima u čijim osmišljavanjima će sudjelovati svi dionici (nastavnici, roditelji, učenici). Osim stručne službe škole i učitelja, u provođenju aktivnosti sudjelovat će i stručnjaci iz udruga i organizacija koje se bave odgojem i obrazovanjem.</p> <p>Pokazatelj ostvarivanja cilja su evidencije održanih aktivnosti, broj sudionika i rezultati vrednovanja koje će se održati u razdoblju od rujna 2017. do lipnja 2022. godine, a dugoročni pokazatelj će biti povećan uspjeh učenika u školskom okruženju, povećana razina povjerenja između obitelji i škole i unaprjeđena suradnja.</p> <p>Za ostvarivanje cilja potrebi su ljudski, organizacijski i dijelom financijski resursi s kojima već raspolažemo. Točnim i jasnim planiranjem aktivnosti i pridržavanjem Godišnjeg plana i programa rada škole i školskog kurikulumu za sljedeće četiri školske godine, cilj je ostvariv u predviđenom vremenskom roku.</p>

Aktivnosti	<ul style="list-style-type: none"> • Analiza okruženja i odabir područja razvoja • Izrada i usvajanje Razvojnog plana škole i smjernica rada • Izrada prijedloga plana aktivnosti za razdoblje rujanj 2018.- lipanj 2023. • Održavanje sjednica Vijeća roditelja, Učiteljskog vijeća i Vijeća učenika (uključivanje u planiranje, konzultacije) • Planiranje i održavanje edukacija za roditelje (teme određene prema razredima), roditeljskih sastanaka, sastanaka na kojima su i učenici i roditelji, kreativnih radionica za roditelje i učenike, izleta i posjeta, izvannastavnih aktivnosti • Tijekom četverogodišnjeg razdoblja omogućiti roditeljima veću dostupnost individualnog savjetodavnog rada sa stručnom službom • Vrednovanje aktivnosti i samovrednovanje na kraju svaku školske godine • Izrada izvješća • Po potrebi izraditi smjernice za rad s roditeljima i učenicima
Nositelji	Tim za kvalitetu, stručna služba, ravnateljica, učitelji informatike
Koordinator	Pedagoginja
Korisnici	Učenici, učitelji, roditelji, lokalna zajednica, lokalna zajednica (udruge, organizacije, ustanove)
Pokazatelji	Izrađeni Školski kurikulumi u razdoblju 2018.- 2023., Razvojni planovi u razdoblju od 2018. do 2023. rezultati vrednovanja i upitnika, evidencija radionica, savjetovanja, školski list
Nositelji i vrijeme praćenja pokazatelja	<ul style="list-style-type: none"> • usvojen Školski kurikulum i Razvojni plan • Lipanj 2018.-2023. rezultati vrednovanja i/ili upitnika • 2018.-2023. usvojen Školski kurikulum i Razvojni plan • 2019.-2022. rezultati i analiza realizacije, vrednovanja i upitnika • Izrada izvješće na kraju svake školske godine

CILJ 2.	Unaprjeđenje sigurnosti učenika na Internetu
Mjera 2.2.	Unaprjeđene IKT kompetencija kod učenika
Cilj i opis mjere	<p>Cilj mjere je:</p> <ul style="list-style-type: none"> • unaprijediti IKT kompetencije učenika • osvijestiti učenike o sigurnom i odgovornom korištenju internetu kroz primjenu aktivnosti projekta Pet za net • Razviti suradnički odnos roditelja i škole <p>Učenici od 1. do 8. razreda će s učiteljicama, razrednicima i učiteljima informatike kroz planirane aktivnosti naučiti kako se sigurno koristiti internetom, komunicirati u online okruženju, zaštititi svoju privatnost, ne ugrožavati i sebe i druge te naučiti koristiti se ITK tehnologijom dostupnoj u školi.</p>
Aktivnosti	<ul style="list-style-type: none"> • formiranje Tima za unaprjeđenje IKT kompetencija • odabir tema iz projekta Pet za net za 4 modula • izrada plana realizacije aktivnosti i tema • provedba radionica, predavanja kroz 2 školske godine • obilježavanje Dana sigurnosti na internetu • obilježavanje Dana otvorenih vrata na temu online okruženja u suradnji s roditeljima • izrada izvješća
Nositelji	učitelji, stručna služba, MUP, civilni sektor
Koordinator	Pedagoginja
Korisnici	Učenici, roditelji, učitelji
Pokazatelji	Kurikulum projekta Pet za net, Godišnji planovi i programi, Kurikulum, web stranica škole, stranica škole na društvenim mrežama, izvješća
Praćenje pokazatelja	Tim za unaprjeđenje IKT kompetencija izrađuje izvješće na kraju školske godine.

X. KORIŠTENJE MOBILNIH TELEFONA

Članak 10.

Kućnim redom škole propisano je da je zabranjeno korištenje mobitela za vrijeme nastave.

U slučaju prekršaja učitelj ima pravo oduzeti učeniku mobitel i pohraniti ga kod sebe, tajništvo ili kod ravnatelja škole. Mobitel, može preuzeti isključivo učenikov roditelj ili skrbnik.

Učenici mogu koristiti mobitel u slobodno vrijeme (mali odmor, veliki odmor) poštujući odredbe Pravilnika i Kućnog reda.

Iznimno, učenici mogu koristiti mobitele (smartphone) za vrijeme nastave kao nastavno pomagalo kada učitelj to zatraži i pravovremeno najavi. Svaka upotreba tehnologije u učionici mora imati unaprijed zadanu svrhu, koja opravdava korištenje tehnologije. Stoga je važno da cilj upotrebe svake mobilne tehnologije u učionici bude učenje nečeg novog ili ponavljanje poznatih stvari na nov i učenicima zanimljiv način.

Škola je dužna upoznati učenika s posljedicama zlouporabe mobitela. Jedan od popularnih oblika nasilja među vršnjacima koji donosi moderno doba tehnologije je i nasilje putem mobitela. Uključuje bilo kakav oblik poruke zbog koje se osoba osjeća neugodno ili joj se tako prijeti – može biti tekstualna, videoporuka, fotografija, poziv – odnosno bilo kakva višestruko slana poruka kojoj je cilj uvrijediti, zaprijetiti, nanijeti bilo kakvu štetu vlasniku mobilnog telefona.

Škola će kroz roditeljske sastanke informirati roditelje o savjetovanju učenika o korištenju mobitela:

- Naglasiti im da budu pažljivi kome daju broj mobitela.
- Neka pažljivo koriste neku od chat usluga preko mobitela.
- Ako dobiju poruku s nepoznatog broja, neka ne odgovaraju.
- Ne trebaju odgovarati ni na poznate brojeve ako se zbog sadržaja poruke osjećaju loše ili neugodno.
- Objasniti djeci kako šala može lako od smiješne postati uvredljivom, i to da, ako su ljuti, mogu učiniti nešto zbog čega poslije mogu požaliti. Istaknite im da budu pažljivi kad šalju poruke drugima.
- Potaknite ih da se prije slanja poruke zapitaju može li ona uvrijediti ili na bilo koji način naštetiti primatelju?
- Postavite pravilo prema kojem nije dopušteno slati fotografije ili videozapise drugih ljudi bez njihova dopuštenja, kao ni slati sadržaje koji mogu uvrijediti druge ljude.
- Ako dijete dobije neprimjerenu poruku, poziv ili je izloženo nasilju, dajte mu podršku i potaknite ga da odmah razgovara s vama ili nekom drugom odraslom osobom u koju ima povjerenja (poput nastavnika, školskog psihologa), kako se problem ne bi pogoršao.
- Ako je riječ o ozbiljnijim oblicima nasilja, osobito zastrašujućim prijetnjama, razmislite o tome da sve prijavite policiji. U takvim slučajevima dobro je sačuvati poruke u

mobitelu, ili negdje drugdje zapisati podatke o datumu, vremenu i sadržaju poruke ili poziva.

Mobilni telefoni sve više imaju potpuni pristup internetu i djeca i mladi koriste fiksne internetske veze kao i mobitele za pretraživanje interneta. Stoga, iste sigurnosne mjere za korištenje interneta postaju važne i za korištenje mobilnih telefona (zaštita osobnih podataka, izbjegavanje štetnih sadržaja, zaštita potrošača, ovisnost o računalnim igrama, i slično).

Članak 10.

Ovaj Pravilnik stupa na snagu danom donošenja na sjednici Školskog odbora održanoj _____.

KLASA: _____

URBROJ: _____

Slatina, _____.

Predsjednica Školskog odbora:

Tomislava Medvedović

Ravnateljica:

Božica Majhen

