

Na temelju članka 58. Statuta osnovne škole Poreč i čl. 118. st. 2. Zakona o odgoju i obrazovanju u osnovnoj i srednjoj školi (Narodne novine br. 87/08., 86/09., 92/10., 105/10., 90/11., 5/12., 16/12., 86/12., 94/13., 152/14., 7/17., 68/18.) Školski odbor Osnovne škole Poreč, donio je na sjednici održanoj dana 30. rujna 2019. godine

## **PRAVILNIK O SIGURNOJ I ODGOVORNOJ UPOTREBI INFORMACIJSKO-KOMUNIKACIJSKE TEHNOLOGIJE U ŠKOLI**

### **I. UVOD**

#### **Članak 1.**

Ljudski i informacijski resursi smatraju se najvažnijim vrijednostima Škole. Stoga je za sigurno rukovanje informacijama potrebno uspostaviti pravila njihova korištenja kao i pravila ponašanja njihovih korisnika.

Rad Škole ovisi o radu školske infrastrukture. Zbog toga, školska računala moraju biti podešena da omoguće neometan pristup i korištenje informacija potrebnih u nastavi i drugim aktivnostima vezanim za rad Škole.

U Školi je potrebna neprekidna edukacija učenika, nastavnika i svih zaposlenika kako bi se mogao održati korak u korištenju informacijsko-komunikacijske tehnologije (u daljnjem tekstu: IKT), kao i s nadolazećim prijetnjama računalnoj sigurnosti.

Svi izrazi koji se u ovom Pravilniku koriste u muškom rodu neutralni su te se odnose i na muške i na ženske osobe.

#### **Članak 2.**

Ovaj Pravilnik vrijedi za sve korisnike IKT Škole.

U Školi je postavljena infrastruktura Hrvatske akademske i istraživačke mreže - CARNet (u daljnjem tekstu: CARNet).

Učenici i zaposlenici moraju se pridržavati uputa za nesmetano i sigurno korištenje IKT-a koje im može dati administrator imenika, administrator resursa ([http://www.carnet.hr/ustanove\\_clanice/administratori\\_skola](http://www.carnet.hr/ustanove_clanice/administratori_skola)) i administrator eDnevnika Škole.

#### **Članak 3.**

Pravilnik o sigurnoj i odgovornoj upotrebi informacijsko-komunikacijske tehnologije dio je sigurnosne politike Škole. Oblikovan je uzimajući u obzir preporuke Izvršne agencije za obrazovanje, audiovizualnu djelatnost i kulturu (u daljnjem tekstu: EACEA/Eurydice), mreže (<http://eurydice.hr>) koja analizira i pruža informacije o

europskim obrazovnim sustavima, a usmjerena je na strukturu i organizaciju obrazovanja u Europi na svim razinama.

Pravilnik je donesen sa svrhom:

- unaprjeđenja sigurnosti školske informatičke opreme i mreže,
- jasnog definiranja načina 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 mlade,
- poticanja aktivnog sudjelovanja djece u radu s IKT-om promovirajući sigurno, odgovorno i učinkovito korištenje digitalnih tehnologija u mrežnoj zajednici,
- propisivanja sankcija u slučaju kršenja odredbi Pravilnika.

Cilj je sigurnosne politike Škole propisati odredbe koje imaju za cilj upravljanje svim primjenjivim aspektima sigurnosti informacijskih sustava. Njime se propisuju obveze i prava korisnika informacijskih sustava, raspodjela odgovornosti, plan održavanja, dokumentiranje sustava itd. Nadalje, sigurnosna politika mora obuhvatiti i područje upravljanja rizicima, incidentima te postupcima kako se oporaviti od incidenta.

Većina mjera zaštite implementirana je od strane davatelja internetskih usluga - CARNet. Njihovi serveri blokiraju sadržaje i stanice sumnjivog karaktera.

## II. OSNOVNE SIGURNOSNE ODREDBE

### Članak 4.

Materijalni i nematerijalni resursi:

- korisnici IKT infrastrukture su učenici, učitelji, stručni suradnici, ravnatelj, ostali zaposlenici i povremeni korisnici,
- kompletna računalna mreža i računalna oprema smatraju se IKT infrastrukturom čiji je vlasnik Škola,
- virtualnim školskim prostorom smatra se školsko mrežno mjesto <http://os-porec.skole.hr> i sva službena školska mjesta na društvenim mrežama te svako mrežno mjesto na kojem se učenici i zaposlenici Škole javljaju kao njeni službeni predstavnici.

### Članak 5.

Načelo povjerljivosti informacija podrazumijeva da informacije moraju biti dostupne samo onome kome su namijenjene. U skladu s time, Škola razlikuje javne, interne i povjerljive informacije:

Skupinu javnih informacija čine one informacije koje opisuju djelatnosti Škole, a njihova javna dostupnost je u interesu Škole. Tu spadaju kontakt podatci Škole, promidžbeni materijal i ostale informacije s mrežne stranice.

- Interne informacije su one koje se odnose na podatke pojedinca (kontakt podatci, fotografija osobe, podatci iz evidencije koju vodi Škola itd.).
- Povjerljive informacije su svi oni podaci za koje postoji obveza čuvanja profesionalne tajne i čija bi zlouporaba ili pristup neovlaštenoj osobi mogli dovesti do štetnih posljedica na cjelokupni integritet osobe.

Škola koristi brojne službene aplikacije u svrhu prikupljanja, obrade i slanja podataka te su navedene informacije povjerljive. Zaposlenici zaduženi za unos podataka obvezni su čuvati povjerljive informacije te iste ne smiju prosljeđivati neovlaštenim osobama. To se odnosi na pristup podacima: e-Dnevnika, e-Matice, računovodstvenih, administrativnih te drugih mrežnih aplikacija i programa koji sadrže osobne podatke zaposlenika ili učenika. Zaposlenici Škole zaduženi za unos i čuvanje navedenih podataka trebaju svoja računala zaštititi lozinkom koju ne smiju davati neovlaštenim osobama jer u suprotnom čine povredu iz radnog odnosa sankcioniranu važećim propisima.

Tuđe osobne podatke zabranjeno je koristiti bez dopuštenja - privole osobe.

#### Članak 6.

Školska oprema mora se čuvati i pažljivo koristiti.

#### Članak 7.

Zaposlenici Škole posjeduju AAI@EduHr elektronički identitet. Sustav AAI@EduHr je autentifikacijska i autorizacijska infrastruktura sustava znanosti i visokog obrazovanja u Republici Hrvatskoj. Elektronički identitet u sustavu AAI@EduHr je virtualni identitet na CARNET mreži kojega dobivaju pojedinačni korisnici iz ustanova članica CARNET-a (učenici, nastavnici i zaposlenici ustanova članica) i koji im omogućuje korištenje CARNET-ovih usluga.

Zaposlenici Škole dužni su koristiti e-mail koji su dobili iz AAI@EduHr sustava (najčešće u obliku [ime.prezime@skole.hr](mailto:ime.prezime@skole.hr)) u službenoj komunikaciji s nadležnim tijelima i drugim institucijama iz sustava znanosti i obrazovanja kao i za sve edukativne svrhe (e-Matica, e-Dnevnik i sl.).

#### Članak 8.

Poslovnu dokumentaciju važnu za poslovanje Škole potrebno je čuvati na zakonom propisan način.

#### Članak 9.

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

Ozbiljniji incidenti prijavljuju se CARNetovom CERT-u, preko obrasca na mrežnoj stranici [www.cert.hr](http://www.cert.hr) (Computer Security Incident Response Team), organizacijskom entitetu koji reagira na računalno-sigurnosne incidente te preventivnim djelovanjem radi na poboljšanju računalne sigurnosti informacijskih sustava.

### III. ŠKOLSKA IKT OPREMA I ODRŽAVANJE

#### Članak 10.

Povezanost školskih računala na Internet je ostvarena žičnim i/ili bežičnim načinom.

Žično su povezani na Internet:

- uredi ravnatelja i administrativnog osoblja
- računala u informatičkom kabinetu (LAN i Internet)
- pojedine učionice u neposrednoj blizini informatičkog kabineta (učionica likovne i glazbene kulture, vjeronauka i matematike pozicioniran točno iznad)

Škola je u cijelosti pokrivena bežičnim signalom s tri različite mreže (SSID), a koje se dostupnošću djelomično preklapaju, a osmišljene su modularno i za različite korisnike:

- bežična mreža za urede ravnatelja i administrativnog osoblja
- skrivena mreža za bežično spajanje svih učionica
- Microsoftova mreža za učenike, učitelje te po potrebi za učionice

Održavanje i sigurnost Microsoftove mreže je definirana Microsoft Wi-Fi Ugovorom sklopljenim između Microsoft Hrvatska d.o.o. i Škole po kojem opremu održava i nadzire Microsoft najmanje 36 mjeseci od instalacije opreme s mogućnošću produljenja ugovora.

Za održavanje ostale mrežne infrastrukture Škola po potrebi koristi vanjske usluge.

Računalni otpad odvozi ovlaštena tvrtka za prikupljanje elektroničkog otpada.

#### Članak 11.

Zaposlenici se sa svojim privatnim ili školskim uređajima autentificiraju svojim korisničkim podacima iz AAI@EduHr.

Zaposlenicima je strogo zabranjeno davati učenicima i drugim korisnicima vlastite zaporce i druge digitalne identitete.

#### Članak 12.

Sva računala u Školi trenutno posjeduju operativni sustav Windows minimalno verzije Windows 7 s instaliranim Office alatima.

Odabir operativnog sustava za instalaciju se određuje prema specifikacijama računala te uz uvjet da postoji tehnička podrška navedenom operativnom sustavu tj. mogućnost ažuriranja sigurnosnim zakrpama.

Svi operativni sustavi u Školi licencirani su i besplatno preuzeti s web portala Centra za preuzimanje Microsoft proizvoda. Portalu ima pristup samo administrator resursa.

### IV.REGULIRANJE PRISTUPA IKT OPREMI

#### Članak 13.

Računalnoj mreži mogu pristupiti zaposlenici Škole, učenici Škole i gostujući učitelji/učenicu Škole. Nitko od navedenih korisnika ne smije ometati i onemogućavati rad školske mreže.

#### Članak 14.

Učenici smiju koristiti računala samo uz dopuštenje zaposlenika. Pristup aplikacijama i internetskim sadržajima određuje isključivo zaposlenik.

Učenici ne smiju instalirati dodatne računalne programe na računala (igrice ili nekakav drugi program) bez odobrenja administratora. Ako se pojavi potreba za instaliranjem dodatnih programa zaposlenik/učenik se mora javiti administratoru resursa.

Svako nepridržavanje ovih pravila ima negativan utjecaj po Školu i može rezultirati disciplinskom mjerom prema zaposleniku Škole ili pedagoškom mjerom prema učeniku Škole sukladno Pravilniku o kriterijima za izricanje pedagoških mjera.

#### Članak 15.

Zaposlenici i učenici koji koriste informatičku opremu moraju se pridržavati navedenih odredbi:

- učionica mora ostaviti uvijek na kraju onako kako su je zatekli,
- računala se obavezno moraju ugasiti nakon uporabe,
- u slučaju kvara računala učenici će obavijestiti predmetnog učitelja, a zaposlenici administratora resursa ili ravnatelja,
- radna mjesta moraju ostati čista i uredna (namješteni tipkovnica, miš, monitor i stolica na svome mjestu), - prozore obavezno zatvoriti, - učionicu zaključati.

#### Članak 16.

Postavke na računalima/tabletima trebaju biti općenite kako bi se nesmetano odvijala ažuriranja operativnog sustava i antivirusnog programa i kako bi sva računala bila ujednačenih postavki što pruža lakše i brže korištenje i održavanje opreme.

Inicijalno se na računalima za ulaz u operativni sustav ne koristi zaporka. Preporuka je da se na računalima koja redovito koristi veći broj nastavnika postave korisnički računi sa zaporkom te korisnički račun Gost bez zaporka za ostale učitelje i stručne suradnike.

U slučaju potrebe za korištenjem korisničke zaporka u nastavku slijede smjernice koje bi bilo poželjno koristiti pri izradi; ne smije biti kraća od šest (6) znakova, mora imati kombinaciju velikih/malih slova, mora imati minimalno jedan broj i jedan poseban znak.

#### Članak 17.

Svi sadržaji na Internetu nisu primjereni za učenike ili nastavu. Iz toga su razloga određeni sadržaji nedostupni učenicima (filtrirani su). Odlukom Ministarstva znanosti i obrazovanja sve osnovne i srednje škole spojene su na CARNetovu mrežu i automatski su uključene u sustav filtriranja nepoćudnih sadržaja.

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

### **IV. SIGURNOST KORISNIKA**

#### Članak 18.

Učenici i zaposlenici dobivaju elektronički identitet u sustavu [AAI@Edu.hr](mailto:AAI@Edu.hr) koji im se daje na čuvanje i korištenje. U slučaju da izgube svoj korisnički račun, učenik ili roditelj obraćaju se administratoru imenika Škole koji im izdaje novu lozinku.

Ukoliko učenik napušta Školu njegov elektronički identitet se odjavljuje iz te ustanove. Učenicima prestaju prava nad elektroničkim identitetom kada završe sa svojim školovanjem.

Zaposlenicima prestaju prava kada završe sa svojim radnim vijekom, tj. odlaskom u mirovinu ili prestankom rada u školskom sustavu.

Učenici i zaposlenici moraju posebno voditi računa o svojem digitalnom identitetu koji su dobili iz sustava [AAI@edu](mailto:AAI@edu) i korisničkih podataka. Svoje podatke moraju čuvati.

Korisnici moraju voditi računa da, prilikom prijave na ona računala i programe koji zahtijevaju prijavu, ne otkriju svoje podatke za prijavu. Isto tako, zaposlenici se prilikom odlaska iz učionice (kada ostavljaju računalo uključeno) obavezno moraju odjaviti iz svih sustava u koje su se prijavili.

#### Članak 19.

Ciljevi mjera informacijske sigurnosti koje se primjenjuju na računalnu mrežu su:

- omogućavanje elektroničke komunikacije,
- neometano korištenje informacija koje su putem računalne mreže dostupni,
- zaštita školske računalne mreže,
- zaštita osjetljivih podataka Škole.

#### Članak 20.

Svaki pojedinac odgovoran je za svoje ponašanje u virtualnom svijetu te se prema drugim korisnicima mora ponašati pristojno, ne vrijeđati ih, niti objavljivati neprimjerene sadržaje.

Za svakog korisnika koji se susreće s Internetom nužno je upoznavanje 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://hrnetiquette.org>.

Škola će ovaj skup pravila učiniti dostupnim svojim učenicima, o tome ih podučiti, te primijeniti vlastitu politiku u skladu s tim pravilima.

#### Članak 21.

Prilikom korištenja i objavljivanja sadržaja na Internetu, korisnici se moraju pridržavati sljedećih uputa:

- svi korisnici moraju znati da su odgovorni za sve što pišu, objavljuju ili komentiraju na Internetu,
- odgovorni korisnici svojim potpisom stoje iza sadržaja koji objave,
- svaki korisnik mora dobro balansirati između privatnih i školskih informacija koje dijele s drugima,
- korisnici moraju biti pažljivi koje podatke objavljuju na Internetu jer time utječu na svoju sigurnost i zaštitu svoje privatnosti,
- poštivati autorska prava, tj. tuđe radove ne smiju prikazivati kao svoje, niti nedozvoljeno preuzimati tuđe radove s Interneta,

- uravnotežiti vrijeme korištenja Interneta, tj. umjerenosti u korištenju.

a) Prilikom korištenja elektroničke pošte moramo se pridržavati ovih uputa:

- Ukoliko ne koristite postupke enkripcije (hardver ili softver), 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. Gotovo 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" zabranjeni su na Internetu. Pristup mreži (ili servisu ili forumu) može vam biti uskraćen.
- 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.
- Ne šaljite velike količine podataka ljudima koji ih nisu zatražili.

b) Mailing liste, news grupe:

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 okrivljujte sistem administratora zbog ponašanja korisnika sistema.
- 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.
- Krivo predstavljanje nije dopušteno.
- Unaprijed provjerite je li oglašavanje dopušteno. Nezatražene reklamne poruke koje se ne tiču teme rasprave će sigurno uzrokovati da dobijete mnogo ljutih odgovora.
- Sadržaj poruke trebao bi proširivati onu na koju se nadovezuje.
- 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:

- 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.
- Pregledajte forum i budite sigurni da započinjete 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.
- Iz naslova mora biti jasno o kojoj se temi radi.
- Naslov teme mora biti kratak i jasan.
- Razmislite prije nego li napišete bilo što. Morate imati valjan razlog za pisanje poruke, a ona mora biti smisljena.
- Pažljivo sročite svoju poruku. Neka bude što jasnija i jednoznačna. Izbjegavajte nesporazume koliko je to moguće.
- 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.
- Uvijek nastojite poštivati temu.
- Kod odgovora (reply), citirajte poruku na koju odgovarate.
- Ukoliko je poruka na koju odgovarate dugačka, citirajte samo bitne dijelove.
- Privatni razgovori na javnom dijelu foruma nisu poželjni. Za njih koristite privatne poruke, ukoliko postoje, ili e-mail.
- Nastojite da vaši potpisi budu što kraći i neupadljivi.
- Nastojite ne stavljati slike u potpise.
- Nikako nemojte otkrivati svoje osobne podatke, adresu, ime škole, telefonske brojeve i slično preko Interneta (na servisima poput Facebooka, Twittera, chatsobe...).

Pravila sigurnog ponašanja na Internetu su:

- Osobne informacije na Internetu nikad se ne smiju odavati.
- Zaporka je tajna i nikad se ne smije nikome reći.
- Ne odgovarajte na zlonamjerne ili prijeteće poruke.
- 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 dobro razmisliti o ljudima koji se primaju za „prijatelje“.
- Potrebno je biti oprezan s izborom fotografija koje se objavljuju na društvenim mrežama.

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. Svaka Creative Commons licenca osigurava davateljima licence i da ih se prizna i označi kao autore djela.

Zaposlenici i učenici potiču se da potpisuju materijale koji su sami izradili koristeći neku licencu te da poštuju tuđe radove. Nipošto tuđe radove ne smiju 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 online 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.

### Članak 23.

Prednost digitalnog sadržaja je da se ne uništava ili mu se ne umanjuje kvaliteta s brojem kopiranja. Ipak, zbog toga 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 jest kopiranje ili preuzimanje autorski zaštićenog materijala poput e-knjige, glazbe ili pak video sadržaja. 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.

## Članak 24.

Računalna mreža postavljena je tako da u potpunosti onemogućava P2P (peer to peer) protokole i filtrira mrežne stranice koje sadrže P2P datoteke. U potpunosti je zabranjeno korištenje popularno zvanih Torrenata.

Obaveze ustanove su:

- Učenike i zaposlenike podučiti o autorskom pravu i intelektualnom vlasništvu.
- Učenike i zaposlenike 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 zaposlenike podučiti o 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 zaposlenike informirati o mogućim posljedicama nelegalnog korištenja, dijeljenja i umnažanja autorski zaštićenih materijala.

## Članak 25.

Internetsko nasilje definira se kao namjerno i opetovano nanošenje štete korištenjem računala, mobitela i drugih elektroničkih uređaja. Nasilje preko Interneta, 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,
- nasilje mobitelom,
- nasilje na chatu,
- nasilje na forumu,
- nasilje na blogu,
- nasilje na web-servisima (društvene mreže),
- svi ostali oblici nasilja preko Interneta,
- 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 i drugih društvenih mreža),
- postavljanje internetske ankete o žrtvi,
- slanje virusa na e-mail ili mobitel,
- slanje uznemirujućih fotografija putem e-maila, MMS-a ili drugih komunikacijskih alata.

## Članak 26.

Nasilje u školama postao je sve veći problem tijekom nekoliko posljednjih godina, a budući da sve više djece koristi Internet i mobilne telefone za komuniciranje, internetsko nasilje „cyberbullying“ postalo je velik problem.

Škola će, prilikom rješavanja problema internetskog zlostavljanja, koristiti sve raspoložive oblike individualne i grupne pomoći i podrške. U težim slučajevima zlostavljanja koji uključuju ozbiljne prijetnje prema drugim učenicima, a rezultiraju time da žrtva više ne želi ići u školu ili pak ako se nasilje nastavi unatoč prethodno poduzetim mjerama savjetovanja, pomoći i podrške, potrebno je izreći pedagošku mjeru sukladno važećim pravilnicima.

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

Edukacija o neprihvatljivom ponašanju provode se kroz predmete koji koriste tehnologiju ili Sat razrednika, te su pravila o prihvatljivom ponašanju i korištenju tehnologije vidljiva i u prostorijama Škole.

Stručna služba Škole provodit će savjetodavni rad s učenicima koji provode razne oblike uznemiravanja, a kroz strategiju će se provesti i preventivne mjere suzbijanja nasilja.

Škola će:

- Podučiti učenike i zaposlenike o mogućim oblicima internetskog nasilja i o tome kako prepoznati internetsko nasilje.
- Jasno istaknuti prihvatljiva pravila ponašanja te učenike i zaposlenike podučiti kroz predmete koji koriste tehnologiju.
- Izraditi strategiju odgovora na internetsko nasilje.
- Obilježavati Dane sigurnog korištenja Interneta i suzbijanja nasilja kroz kreativne radove.

## Članak 27.

S ciljem unaprjeđenja suradnje s roditeljima, predviđeno je povećano sudjelovanje roditelja u školskim aktivnostima u području IKT tehnologije. 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.

Roditelji će navedene ciljeve razvijati kroz sudjelovanje na sastancima, individualnim razgovorima, razrednim projektima, školskim projektima, edukacijama za roditelje o sigurnosti na Internetu, korištenju e-dnevnika i sl., izvannastavnim aktivnostima.

## Članak 28.

Kućnim redom Škole propisano je da je zabranjeno korištenje mobitela u vrijeme nastave, školskih odmora, u unutarnjem prostoru Škole te u njenom okolišu.

U slučaju prekršaja zaposlenik ima pravo oduzeti učeniku mobitel i predati ga tajniku ili ravnatelju Škole. Mobitel može preuzeti isključivo učenikov roditelj ili skrbnik.

Učenici mogu iznimno koristiti mobitele za vrijeme nastave kao nastavno pomagalo u dogovoru s predmetnim nastavnikom. Svaka upotreba tehnologije u učionici mora imati unaprijed zadanu svrhu koja opravdava korištenje tehnologije.

#### Članak 29.

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 je dužna upoznati učenika s posljedicama zlouporabe mobitela te da je svaki oblik nasilja kažnjiv zakonom.

Ukoliko Škola ima saznanja o bilo kojem obliku nasilja postupit će sukladno odredbama zakona te u suradnji s nadležnim institucijama i tijelima pokrenuti postupak radi zaštite prava učenika.

#### Članak 30.

Škola će kroz roditeljske sastanke informirati roditelje 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
- Postaviti 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 ili školskog suradnika) 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 imaju sve više 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 programima i slično).

#### Članak 31.

Ovaj Pravilnik objavit će se na mrežnim stranicama i oglasnoj ploči Škole.  
Pravilnik stupa na snagu osmog dana od dana objave na oglasnoj ploči Škole.

KLASA:003-05/19-01/05

URBROJ: 2167-23-01-19-1

U Poreču, 30. rujna 2019. godine

Predsjednica Školskog odbora:

Martina Vladišković-Bernobić, prof.

#### OBJAVA PRAVILNIKA

Ovaj Pravilnik objavljen je na oglasnoj ploči Škole 30. rujna 2019. godine i stupio je na snagu dana 7. listopada 2019. godine.

Ravnateljica:

Nadija Kos, dipl. uč.

