OŠ „PETAR ZRINSKI“ ČABAR
Narodnog oslobođenja 5
51306 Čabar

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

Čabar, 28. siječnja 2021.godine

Na temelju članka 80. Statuta OŠ „Petar Zrinski" Čabar, Školski odbor na sjednici održanoj dana 28. siječnja 2021. godine donio je:

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

UVOD

Članak 1.

Ljudski i informacijski resursi smatraju se najvažnijim vrijednostima OŠ „Petar Zrinski" Čabar, Narodnog oslobođenja 5, 51306 Čabar, OIB: 45593319959, (u daljnjem tekstu: Škola). 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 tako 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.

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 osoba zadužena za podršku uporabi IKT i elektroničkih upisnika (e-Matica, e-Dnevnik i sl.)

Članak 3.

Pravilnik o sigurnoj i odgovornoj upotrebi informacijsko-komunikacijske tehnologije dio je sigurnosne politike Škole.

Pravilnik je donesen sa svrhom:

- unapređenja 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 nasilja
- 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,
- razvijanja digitalnih kompetencija
- 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 incidenata.

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

OSNOVNE SIGURNOSNE ODREDBE

Članak 4.

Materijalni i nematerijalni resursi:

- korisnici IKT infrastrukture su učenici, učitelji, 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-pzrinski-cabar.skole.hr/, a službena školska mjesta na društvenim mrežama te svako mrežno mjesto na kojem se učenici i zaposlenici Škole javljaju kao njeni službeni predstavnici i školske platforme.

Članak 5.

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

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 podatcima: 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 prema načelu dobroga gospodara.

Članak 7.

Zaposlenici Škole posjeduju AAI@EduHr korisnički račun. Sustav AAI@EduHr je autentikacijska i autorizacijska infrastruktura sustava znanosti i visokog obrazovanja u Republici Hrvatskoj.
Zaposlenici su dužni koristiti e-mail (ime.prezime@skole.hr) u službenoj komunikaciji s nadležnim tijelima i drugim institucijama iz sustava znanosti i obrazovanja 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 vevw.cen.hr (Computer Security Incident Response Team), organizacijskom entitetu koji reagira na računalno-sigurnosne incidente te preventivnim djelovanjem radi na poboljšanju računalne sigurnosti informacijskih sustava.

Članak 10.

Računala Škole i računala na korištenje u projektu „e- Škole: Uspostava sustava razvoja digitalno zrelih škola (pilot projekt)"koriste MS Windows operativne sustave, antivirusnu zaštitu, vatrozid i ostale programe odobrene od strane Ministarstva znanosti i obrazovanja. Prema licenčnim ugovorima između MZO i tvrtke Microsoft s MSCD portala po potrebi te programe preuzima osoba s administratorskim ovlastima u Školi. Svi računalni programi moraju se koristiti u skladu s propisima i pripadajućim licencama.

Korisnici resursa koji se spajaju na računalnu mrežu vlastitim pametnim telefonima ili vlastitim tabletima nemaju zaštitu od strane škole.

ŠKOLSKA IKT OPREMA I ODRŽAVANJE

Članak 11.

Računalna mreža je skupina od 2 ili više međusobno povezanih računala. Računala u Školi su povezana žičano i/ili bežično. Škola koristi usluge tvrtke koja je zadužena i plaćena za održavanje navedene mrežne infrastrukture.

Računalni otpad odvozi ovlaštena tvrtka za prikupljanje elektroničkog otpada.

Članak 13.

U sklopu pilot projekta e- Škole imenuje se e- Škole tehničar koji je zadužen za održavanje navedene mrežne infrastrukture. E – škole tehničar imenovan je po naputku osnivača (Primorsko- goranske županije).

Članak 14.

Unutar mreže pilot projekta e- Škole računala i uređaji koji se spajaju bežično spajaju se putem bežičnih pristupnih točaka. Pristupne točke su smještene prema dokumentaciji pilot projekta e – Škole. U bežičnim pristupnim točkama su postavljena tri naziva za pristup bežičnoj mreži

(SSID):

a) Eduroam,

b) eSkole,

c) Quest.

Članak 15.

Na svim računalima u Školi instaliran je operativni sustav MS Windows te MS Office programski paket jer škola putem licenčnih ugovora između MZO i tvrtke Microsoft ima pravo na besplatno korištenje Microsoftovih programa obuhvaćenih ugovorom.

Navedene programe s MSCD portala po potrebi preuzima osoba s administratorskim ovlastima u Školi.

Svi računalni programi moraju se koristiti u skladu s propisima i pripadajućim licencama.

Ukoliko licenčni ugovori ne budu produženi Škola će posebnom odlukom regulirati korištenje operacijskih sustava i programskih paketa.

Svi ostali programi na računala u Školi za potrebe pripreme ili izvođenje nastave, te za poslovanje škole mogu se instalirati isključivo u dogovoru s administratorom resursa.

U računalnoj učionici o instalaciji i pravilnoj uporabi programa brine i odgovoran je voditelj informatičke učionice.

Članak 16.

Računala i uređaji spojeni na Internet kroz računalne mreže Škole koriste CARNet-ovu uslugu filtriranja neprihvatljivih sadržaja s interneta.

Svim korisnicima IKT opreme i infrastrukture zabranjeno je zaobilaženje lozinki ili filtriranja sadržaja.

Članak 17.

Svako nepridržavanje ovih pravila može rezultirati disciplinskim mjerama prema djelatnicima Škole ili pedagoškim mjerama prema učenicima.

Članak 18.

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

Članak 19.

Računala u Školi spojena su žičanim i/ili bežičnim načinom spajanja na mrežu.

Žičano i/ili bežično su spojena sva računala u knjižnici, učionicama te u uredima.

Postavke na računalima koje koriste učenici podešene su na općenite te je na svim računalima postavljeno da kod prijave u operativni sustav nema zaporke. Svi operativni sustavi u Školi licencirani su i besplatno preuzeti od Ministarstva znanosti i obrazovanja.

REGULIRANJE PRISTUPA IKT OPREMI

Članak 20.

Računalnoj mreži mogu pristupiti učenici, učitelji, ostali djelatnici škole te vanjski partneri i posjetitelji. Ovisno o statusu u Školi i namjeni uređaja priključuju se na jednu od tri bežične mreže (SSID):

1. ESkole- služi za povezivanje tableta u STEM učionicama na bežičnu mrežu, odnosno za povezivanje uređaja koje koristi više različitih osoba (učenici i učitelji prilikom spajanja identificiraju se korisničkim podacima iz AAI@EduHr sustava što omugućava identifikaciju i praćenje prometa u računalnoj mreži),
2. Eduroam- služi za povezivanje učenika, učitelja i ostalog osoblja na bežičnu mrežu, odnosno za povezivanje uređaja kojeg u pravilu koristi samo jedna osoba (učenici i učitelji spajaju se svojim privatnim ili školskim uređajima),
3. Quest- služi za povezivanje vanjskih posjetitelja i partnera na bežičnu mrežu (to je mreža otvorenog tipa, a e- Škole tehničar mora kreirati korisničko ime za svakog korisnika kojem Škola odobri pristup mreži).

Nitko od navedenih korisnika ne smije ometati i onemogućavati rad školske žičane ili bežične mreže.

Članak 21.

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.

Članak 22.

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

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

Članak 23.

Većina računala u školi podešena su da se za ulaz u operativni sustav ne koristi zaporka.

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

Članak 24.

Nisu svi sadržaji na Internetu 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.

Članak 25.

Ako učenici na IKT opremi u Školi primijete neprimjerene, uznemirujuće ili sadržaje koji ugrožavaju sigurnost, o tome odmah trebaju obavijestiti učitelje ili ravnatelja.

Članak 26.

Nadzor mrežnog prometa vrši tehničar e-Škole.

SIGURNOST KORISNIKA

Članak 27.

Učenici dobivaju elektronički identitet u sustavu 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 daje novu lozinku.

Ukoliko učenik napušta Školu, njegov elektronički identitet se briše. 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.hr. 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 28.

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

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

Članak 29.

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

httHYPERLINK "http://hr-netiquette.org/"p://hr-netiquette.org.

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

Članak 30.

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 (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. 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.
- 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 ljutitih odgovora.
- Sadržaj poruke trebao bi proširivati onu na koju se nadovezuje.
- Predstavljanje tuđim imenom u news člancima nije dopušteno. Od toga se možete zaštiti korištenjem softwarea kao što je PGP („Pretty Good Privacy").

c) Forumi:

- Ako postoje pravila foruma, obavezno ih pročitajte i 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 smislena.
- 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 nastojte 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.
- Nastojte da vaši potpisi budu što kraći i neupadljivi.
- Nastojte 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, chat-sobe...).

- e okrivljujte sistem administratora zbog ponašanja korisnika sistema.

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.

Članak 31.

Autorska prava na online-dokumentima najčešće se definiraju s tzv. Creative Commons (CC) licencama (više na :

https://creativecommons.org/licenses/?laHYPERLINK"https://creativecommons.org/licenses/?lang=hr"ng=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 niti preuzimati zasluge za tuđe radove.

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 32.

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, video sadržaja 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 video sadržaji 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 33.

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 onemogućeno korištenje popularno zvanih Torrenata.

Obaveze ustanove su:

1. Učenike i zaposlenike podučiti o autorskom pravu i intelektualnom vlasništvu.

2. 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.

3. 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.

4. Učenike i zaposlenike informirati o mogućim posljedicama nelegalnog korištenja, dijeljenja i umnažanja autorski zaštićenih materijala.

Članak 34.

Elektroničko 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 elektroničkog nasilja:

- 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 35.

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, elektroničko nasilje postalo je velik problem.

Škola će, prilikom rješavanja problema elektroničkog nasilja, 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:

1. Podučiti učenike i zaposlenike o mogućim oblicima elektroničkog nasilja i o tome kako prepoznati elektroničko nasilje.

2. Jasno istaknuti prihvatljiva pravila ponašanja te učenike podučiti kroz predmete koji koriste tehnologiju, a zaposlenike kroz razne oblike edukacije.

3. Izraditi strategiju odgovora na elektroničko nasilje

4. Obilježavati Dane sigurnog korištenja Interneta i suzbijanja nasilja kroz kreativne radove.

Članak 36.

S ciljem unaprjeđenja suradnje s roditeljima, razrednici će na satovima razrednika i na roditeljskim sastancima upoznati učenike i roditelje sa školskim aktivnostima u području IKT.

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, materijalima objavljenim na mrežnoj stranici Škole.

Članak 37.

Kućnim redom Škole propisano je da je zabranjeno korištenje mobitela u prostoru Škole, uključujući i dvorište između Škole i dvorane.

U slučaju prekršaja, zaposlenik ima pravo oduzeti učeniku mobitel. Mobitel može preuzeti isključivo učenikov roditelj ili skrbnik.

Učenici mogu koristiti mobitel izvan prostora Škole uključujući školsko dvorište.

Učenici mogu koristiti školske tablete 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 38.

S obzirom da mobilni telefoni sve više imaju potpuni pristup internetu te da djeca i mladi koriste fiksne internetske veze kao i mobitele za pretraživanja interneta, 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).

Škola će upoznati učenika s posljedicama zlouporabe mobilnih telefona. Najrašireniji oblik nasilja među vršnjacima je nasilje putem mobilnih telefona.

Ono uključuje bilo kakav oblik poruke zbog koje se osoba osjeća neugodno ili joj se tako prijeti (tekstualna poruka, video poruka, fotografija, poziv) odnosno kojoj je cilj uvrijediti, zaprijetiti, nanijeti bilo kakvu štetu vlasniku mobilnog telefona.

Članak 39.

Škola će kroz roditeljske sastanke, individualne informacije i putem mrežnih stranica škole informirati roditelje o sigurnom korištenju IKT-a kod djece:

- 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.
- Potaknuti 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, dati mu podršku i potaknuti ga da odmah razgovara s vama ili nekom drugom odraslom osobom u koju ima povjerenja (poput učitelja ili školskog stručnog suradnika) kako se problem ne bi pogoršao.
- Ako je riječ o ozbiljnijim oblicima nasilja, osobito zastrašujućim prijetnjama, razmisliti o tome da se sve prijavi 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 40.

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

Ovaj Pravilnik objavit će se na mrežnim stranicama Škole te stupa na snagu i primjenjuje se s danom objave.

KLASA: 011-03/21-01/01
URBROJ: 2108-19-01-21-02

Predsjednik Školskog odbora:
Marijo Stojak, dipl.theol.
Marijo Stojak

Ravnateljica:
Silvana Šebalj Mačkić mag.prim.educ.