

DRVODJELJSKA ŠKOLA ZAGREB
Savska cesta 86
10 000 ZAGREB

**PRAVILNIK O SIGURNOJ I ODGOVORNOJ
UPOTREBI INFORMACIJSKO-
KOMUNIKACIJSKE TEHNOLOGIJE
DRVODJELJSKE ŠKOLE ZAGREB**

Zagreb, 2020.

Na temelju odredbe članka 28. Statuta Drvodjeljske škole Zagreb, KLASA: 602-01/19-01/5; URBROJ:251-87-01-19-1 od 10. siječnja 2020. godine te odredbe članka 118. stavka 2. Zakona o odgoju i obrazovanju u osnovnoj i srednjoj školi (NN 87/08, 86/09, 92/10, 105/10, 90/11, 5/12, 16/12, 86/12, 126/12, 94/13, 152/14, 07/17, 68/18 i 98/19) Školski odbor Drvodjeljske škole Zagreb, a na prijedlog ravnateljice Drvodjeljske škole Zagreb, Školski odbor Drvodjeljske škole Zagreb na sjednici održanoj 03.06. 2020. godine donosi

PRAVILNIK O SIGURNOJ I ODGOVORNOJ UPOTREBI INFORMACIJSKO-KOMUNIKACIJSKE TEHNOLOGIJE DRVODJELJSKE ŠKOLE ZAGREB

I. UVOD

Članak 1.

S obzirom na sve veću sustavnu upotrebu informacijsko-komunikacijske tehnologije (dalje u tekstu: IKT) 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 posvetiti sigurnom i odgovornom korištenju IKT-a, a što je moguće postići definiranjem sigurne politike škole.

Svrha Pravilnika o sigurnoj i odgovornoj upotrebi informacijsko-komunikacijske tehnologije Drvodjeljske škole Zagreb (dalje u tekstu: Pravilnik) je:

- Unaprjeđenje sigurnosti školske informatičke opreme i mreže.
- Jasno i nedvosmisleno određivanje načina prihvatljivog i dopuštenog korištenja IKT resursa škole.
- Zaštita informacijskog sadržaja i opreme.
- Promoviranje sustava i usluga najprikladnijih učenicima.
- Poticanje aktivnog sudjelovanja učenika u radu s IKT-om promovirajući sigurno, odgovorno i učinkovito korištenje digitalnih tehnologija.
- Propisivanje sankcija u slučaju kršenja odredaba Pravilnika.

Ovaj Pravilnik primjenjuje se na sve korisnike IKT infrastrukture Škole.

Članak 2.

U Školi je u siječnju 2019. godine postavljena infrastruktura LAN i Wireless mreže naslonjena na dobavljača interneta CARNET. Radove je izvela tvrtka Alarm Automatika d.o.o. Neposredni učesnik je bio nastavnik računalstva Tihomir Pauković.

Učenici su dužni pridržavati se uputa koje im daju nastavnici ili druge ovlaštene osobe, a kojima je cilj unapređenje sigurnosti školske informatičke opreme i mreže.

II. OSNOVNE SIGURNOSNE ODREDBE

Članak 3.

Kompletna računalna mreža izgrađena te postojeća i nova računalna oprema dobivena projektom Informatizacije škole se smatra IKT infrastrukturom Škole.

Korisnici IKT infrastrukture su učenici, nastavnici, ostali djelatnici i povremeni korisnici (gosti).

Materijalni resursi su:

- Kompletna računalna mreža izgrađena u sklopu projekta Informatizacija škole i računalna oprema.
- Stara računalna oprema.

Nematerijalni resursi su:

- Aplikacije koje škola koristi: e-dnevnik, e-matica, Obračun plaća s evidencijom kadrova.

Članak 4.

Školska oprema se mora čuvati i pažljivo koristiti. Korisnici ne smiju uništavati IKT infrastrukturu škole. Svaki radnik pri preuzimanju opreme na korištenje potpisuje zadužnicu kojom se obvezuje po prestanku korištenja vratiti opremu u ispravnom stanju, a u suprotnom odgovara za nastalu štetu.

Članak 5.

U poslovanju Škole razlikujemo javne i povjerljive informacije. Javne su one informacije koje su vezane uz djelatnost Škole i čija je javna dostupnost u interesu Škole (kontakt podaci Škole, promidžbeni materijali, internetske stranice Škole, informacije koje je Škola u skladu sa zakonom dužna objavljivati i sl.).

Povjerljive informacije su osobni podaci djelatnika, učenika (npr. kontakt podaci osobe, fotografije osobe,...), podaci iz evidencija koje vodi Škola (e-Dnevnik, e-Matica, matične knjige,...) te informacije koje se smatraju poslovnom tajnom.

Tudi osobni podaci se mogu koristiti isključivo uz prethodno odobrenje ravnatelja ili osobe koju on za to posebno opunomoći.

Članak 6.

Računala koja su na Windows operativnim sustavima (Windows 7, 8 i 10) posjeduju antivirusni program.

Učenici, nastavnici i ostali djelatnici koji se spajaju na računalnu mrežu vlastitim pametnim telefonima čiji su sustavi Android, Windows i OS, nemaju zaštitu od strane škole.

Na računalima u informatičkoj učionici mjera zaštite je implementirana kod davatelja internetskih usluga. Njihovi serveri blokiraju sadržaje i stranice sumnjivog karaktera.

Članak 7.

Djelatnici Škole posjeduju AAI@EduHr korisnički račun te su dužni koristiti službenu e-mail adresu (ime.prezime@skole.hr) za komunikaciju s nadležnim tijelima i institucijama iz sustava znanosti i obrazovanja..

Članak 8.

Nastavnicima i drugim djelatnicima Škole zabranjeno je davati učenicima i drugim korisnicima vlastite zaporke i digitalne identitete.

Članak 9.

Svi djelatnici Škole koji zbog prirode posla imaju pristup osobnim podacima ostalih osoba dužni su pridržavati se važećih propisa i etičkih načela iz područja zaštite osobnih podataka te na zahtjev škole potpisati izjavu o tajnosti podataka.

Članak 10.

Svako nepridržavanje ovih pravila 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.

III. ŠKOLSKA IKT OPREMA I ODRŽAVANJE

Članak 11.

Računala u školi su povezana bežično i žičano. Računalna mreža se sastoji od novog dijela koje je izgrađen u sklopu projekta Informatizacija škole te starog dijela mreže (router CARNET). Računalni otpad zbrinjava se odvojeno od ostalog otpada, a Škola će takav otpad predati ili sama odvesti ovlaštenom sakupljaču EE otpada.

Članak 12.

Računala se bežično spajaju na 15 bežičnih pristupnih točaka. Pristupne točke su smještene u svakom holu i školskoj radionici. U bežičnim pristupnim točkama su postavljena četiri naziva za pristup bežičnoj mreži (SSID):

- a) Drvodjeljska_skola_Zagreb,
- b) Drvodjeljska_skola_Zagreb_5G,
- c) Drvodjeljska_gost,
- d) Drvodjeljska_gost_5G

Članak 13.

Sva računala u Školi posjeduju operativni sustav Windows s instaliranim Office alatima. Računala u informatičkoj učionici posjeduju Windows 7 i Windows 10 operativni sustav s instaliranim Office 2007 alatima. Postavke na računalima su podešene na općenite te je na svim računalima postavljeno da kod prijave u operativni sustav koriste zaporku. Također, uključena je opcija da lozinka nikada ne ističe (Password never expires). Kod svih računala je podešeno ažuriranje operativnog sustava i popratnih office alata na „automatski“. Računalna mreža pokazuje da najviše prometa koja računala ostvaruju preko interneta odlazi baš 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. Operativni sustavi Windows 7 imaju u sebi obrambeni sustav (Windows Essentials Security) te također i vatrozid koji posjeduju i stariji operativni sustavi do Windows XP-a.

Članak 14.

Škola koristi računalne programe licencirane od strane Ministarstva znanosti i obrazovanja i tvrtke Microsoft. Ministarstvo znanosti i obrazovanja je izradilo web portal Centar za preuzimanje Microsoft proizvoda. Portalu imaju pristup svi odgovorni za održavanje i instalaciju računalnih programa u školama (administratori sustava).

U sustav se prijavljuje AAI@edu korisničkim računom gdje se mogu preuzeti svi navedeni operativni sustavi i office alati s pripadajućim ključevima za aktivaciju.

Svi programi koji su instalirani i korišteni na uređajima moraju imati važeću licencu te se moraju upotrebljavati u skladu s važećim propisima i pripadajućim licencama. Ako se netko koristi nelegalnim softverom ili softverom koji je instalirao bez dopuštenja osobno snosi posljedice, a osoba odgovorna za održavanje opreme nije dužna popraviti štetu koja je nastala upotrebom neovlašteno instaliranog softvera.

Za sva računala i programe koji su dodijeljeni nastavnicima u sklopu projekta e-Škole odgovorne su isključivo te zadužene osobe, kao i za programe na školskim računalima koji jer svi programi koji se instaliraju i koriste moraju imati važeću licencu te se moraju upotrebljavati u skladu s važećim propisima i licencama.

Škola koristi računalne programe AutoCad od strane tvrtke Autodesk sa slobodnim licencama - education.

Članak 15.

Učenici ne smiju instalirati nikakve računalne programe u informatičkoj učionici (igrice ili sl.).

Na ostala računala u Školi nije dopušteno ništa instalirati bez odobrenja administratora. Ukoliko se pojavi potreba za instaliranje dodatnog računalnog programa, djelatnik odnosno učenik koji ga želi instalirati dužan je obvezno se javiti administratoru.

Članak 16.

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

IV. REGULIRANJE PRISTUPA IKT OPREMI

Članak 17.

Računalnoj mreži mogu pristupiti učenici, nastavnici, 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 četiri naziva za pristup bežičnoj mreži (SSID):

- a) Drvodjeljska_skola_Zagreb,
- b) Drvodjeljska_skola_Zagreb_5G,
- c) Drvodjeljska_gost,
- d) Drvodjeljska_gost_5G

a) Na Drvodjeljska_skola_Zagreb se spajaju nastavnici sa svojim privatnim ili školskim uređajima.

b) Na Drvodjeljska_skola_Zagreb_5G se spajaju nastavnici sa svojim privatnim ili školskim uređajima.

c) Drvodjeljska_gost, mreža se koristi za spajanje učenika i vanjskih partnera i posjetitelja.

d) Drvodjeljska_gos_5G, mreža se koristi za spajanje učenika i vanjskih partnera i posjetitelja.

U sklopu projekta e-Škole, nastavnici i stručni suradnici zaduženi su opremom (prijenosna računala).

U slučaju duže odsutnosti djelatnika, a u svrhu normalnog funkcioniranja nastavnog procesa, djelatnik je dužan vratiti opremu, o čemu odluku donosi ravnatelj.

Članak 18.

Učenici smiju uz dopuštenje nastavnika koristiti samo školska računala koja su njima namijenjena (računala u informatičkoj učionici).

Vlastita računala i pametne telefone učenici smiju za vrijeme nastave koristiti isključivo u obrazovne svrhe i uz prethodnu dozvolu nastavnika, pri čemu moraju paziti da ne ugrožavaju

druge korisnike školske mreže širenjem virusa i drugih zlonamjernih programa. Kojim aplikacijama i internetskim sadržajima učenici mogu pristupiti određuje isključivo nastavnik.

Učenici smiju koristiti vlastita računala u privatne svrhe isključivo za vrijeme odmora te prije i poslije nastave.

Učenici su dužni svaki uočeni kvar (hardverski ili softverski) prijaviti nastavniku te ne smiju samovoljno popravljati računala.

Članak 19.

Osim računalima koja su dobili u sklopu pilot projekta e-Škole nastavnici imaju pristup računalima u zbornici te, prema potrebi, računalima u informatičkoj učionici, a ostalo osoblje računalima u uredima Škole.

Članak 20.

Svi nastavnici koji koriste informatičku učionicu moraju se pridržavati sljedećih naputaka:

- Učionica mora ostati na kraju onako kako je i zatečena.
- Računala se obavezno moraju ugasiti nakon uporabe.
- U slučaju da neko od računala ne radi treba kontaktirati nastavnika informatike (voditelja informatičke učionice).
- Radna mjesta moraju ostati uredna (namještena tipkovnica, miš, monitor, stolica na svojem mjestu).
- Prozore obavezno zatvoriti.
- Učionicu zaključati.

Nastavnik informatike (voditelj informatičke učionice) je odgovoran za informatičku učionicu.

Članak 21.

U Školi su sva računala podešena tako da se za ulaz u operativni sustav koristi zaporka. Također je uključena opcija u operativnom sustavu da loznika nikada ne prestaje (Password never expires).

Preporučuje se korištenje korisničkih zaporki koje se sastoje od kombinacije malih i velikih slova, brojeva i posebnih znakova te su minimalne duljine 6 znakova.

Članak 22.

Odlukom Ministarstva znanosti i obrazovanja sve osnovne i srednje škole spojene na CARNet mrežu automatski su uključene i u sustav filtriranja nepoćudnih sadržaja.

Od učenika se očekuje da prihvate filtriranje određenih sadržaja kao sigurnosnu mjeru te ga ne smiju pokušati zaobići, jer je ono postavljeno radi njihove sigurnosti, ali i sigurnosti svih drugih učenika. Nadalje, zaobilaženje sigurnosnih postavki moglo bi ugroziti održavanje nastave.

Ako učenik smatra da je određeni sadržaj neopravdano blokiran ili propušten može se obratiti nastavniku informatike. Ako učenici primijete neprimjerene, uznemirujuće ili sadržaje koji ugrožavaju njihovu sigurnost, o tome odmah trebaju obavijestiti nastavnike ili ravnatelja.

V. SIGURNOST KORISNIKA

Članak 23.

U Školi je potreba neprekidna edukacija učenika, nastavnika i ostalih djelatnika da bi se mogao održati korak u korištenju IKT-a, kao i s nadolazećim prijetnjama u računalnoj sigurnosti. Prilikom korištenja računala i programi koji zahtjevaju prijavu lozinkom, potrebno je voditi računa da se kod prijave ne otkriju podaci o prijavi. Kada učenici odlaze iz učionice, a ostavljaju računalo uključeno, nastavnici su dužni odjaviti ih iz svih sustava u koje su se prijavili.

Također, učenici koji koriste računala u računalnim učionicama, dužni su se obvezno nakon završetka rada odjaviti iz sustava u koje su se prijavili.

Članak 24.

Korisnici su dužni posebno voditi računa o svojem elektroničkom identitetu koji su dobili iz sustava AAI@edu. Svoje podatke moraju čuvati.

Početkom školovanja u Školi svi učenici dobivaju elektronički identitet u sustavu AAI@EduHr. U slučaju gubitka korisničke oznake ili zaporke, odnosno u slučaju da mu je zaključan elektronički identitet, učenik se treba javiti administratoru imenika. Kada učenik prelazi u Školu iz druge škole, njegov elektronički identitet se prenosi.

Minimalno jednom godišnje (početkom školske godine) potrebno je revidirati elektroničke identitete učenika.

Nakon isteka učeničkog statusa i prestanka potrebe za posjedovanjem elektroničkog identiteta učenika, identitet je potrebno isključiti.

Pri zapošljavanju novog djelatnika, administrator imenika dodjeljuje mu elektronički identitet u sustavu AAI@EduHr, a pri prestanku radnog odnosa, identitet je potrebno isključiti.

Pravila pristupa učenika i djelatnika Škole školskim računalima potrebno je redovito provjeravati i po potrebi mijenjati.

Članak 25.

Datoteke preuzete iz nekog vanjskog izvora (putem elektroničke pošte, vanjskog diska, ili interneta) mogu ugroziti sigurnost učenika odnosno nastavnika. Zato je uputno ne otvarati ili prosljeđivati zaražene datoteke i programe kao niti otvarati datoteke iz sumnjivih ili nepoznatih izvora. Sve takve datoteke potrebno je provjeriti antivirusnim alatom prije korištenja

VI. PRIHVATLJIVO I ODGOVORNO KORIŠTENJE INFORMACIJSKO-KOMUNIKACIJSKE TEHNOLOGIJE

Ponašanje na internetu

Članak 26.

Korisnici školskih računala odgovorni su za svoje ponašanje u virtualnom svijetu te se prema drugim korisnicima moraju ponašati pristojno, ne vrijeđati ih, niti objavljivati neprimjerene sadržaje.

Škola će korisnike upoznati s pravilima poželjnog ponašanja na internetu, objavljivanjem navedenih pravila u informatičkoj učionici.

Članak 27.

Učenike se na nastavi informatike i satu razredne zajednice poučava osnovnim pravilima ponašanja u virtualnom svijetu (ne otkrivati osobne podatke, svoju adresu, ime škole, telefonske brojeve i slično preko interneta na servisima poput Facebooka, Twitera, chat sobe...).

Članak 28.

Osim Pravila poželjnog ponašanja na internetu, uputno je da se učenici pridržavaju i sljedećih naputaka (Pravila sigurnog ponašanja):

- Osobne informacije na internetu se nikad ne smiju odavati.
- Zaporka je tajna i nikad se ne smije nikome reći.
- Ne odgovaraju 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.
- Treba 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).

Autorsko pravo

Članak 29.

Korisnike se potiče da potpisuju materijale koje su sami izradili, ali i da poštuju tuđe radove. Nipošto ne smiju tuđe radove predstavljati kao svoje, preuzimati zasluge za tuđe radove, niti nedozvoljeno preuzimati tuđe radove s interneta. Korištenje tuđih materijala s interneta mora biti citirano, obavezno navodeći autora korištenih materijala te izvor informacije (poveznica i datum preuzimanja). Svaki korisnik odgovaran je za poštivanje autorskog prava i intelektualnog vlasništva.

Za fotografiranje i snimanje tuđih radova (prezentacija, plakata, tiskanih materijala) potrebno je imati dozvolu autora rada odnosno privolu.

Članak 30.

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

Članak 31.

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.

Dijeljenje datoteka

Članak 32.

Pri korištenju digitalnih sadržaja, a osobito pri njihovu dijeljenju treba biti osobito oprezan.

U Školi je izričito zabranjeno nelegalno dijeljenje datoteka (npr. kopiranje ili preuzimanje autorski zaštićenog materijala poput e-knjige, glazbe ili pak videosadržaja).

Učenike i nastavnike treba podučiti o autorskom pravu i intelektualnom vlasništvu te ih usmjeriti na korištenje licenci za zaštitu autorskog prava i intelektualnog vlasništva.

Učenike i nastavnike treba podučiti o načinima nelegalnog dijeljenja datoteka i servisima koji to omogućuju (npr. Torrent).

Učenike i nastavnike treba informirati o mogućim posljedicama nelegalnog korištenja, dijeljenja i umnažanja autorski zaštićenih materijala.

Internetsko nasilje

Članak 33.

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

Postoje različiti oblici internetskog zlostavljanja:

- nastavljanje slanja e-pošte usprkos tome što netko više ne želi komunicirati s pošiljateljem,
- 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.

Članak 34.

Nedopušteni su svi oblici nasilničkog ponašanja te će svi oni za koje se utvrdi da provode takve aktivnosti disciplinski odgovarati.

Potrebno je učenike i nastavnike podučiti o mogućim oblicima internetskog nasilja te o tome kako prepoznati internetsko nasilje.

U Školi je potrebno razviti nultu stopu tolerancije na internetsko nasilje.

Svi korisnici, a posebno učenici, moraju znati da su odgovorni za sve što pišu, objavljuju ili komentiraju na internetu te trebaju biti svjesni publike (kolege, potencijalni poslodavci, suradnici i sl.). Potrebno ih je osvijestiti i promišljenom dijeljenju svojih osobnih podataka, jer jednom objavljen podatak više nije moguće trajno otkloniti.

Fotografiranje i snimanje osoba smije se napraviti samo uz prethodno dopuštenje. Potrebno je imati i dopuštenje za objavu takvih digitalnih sadržaja.

Prilikom dijeljenja privatnih i školskih informacija korisnici se trebaju voditi načelima otvorenosti i transparentnosti te zaštite privatnosti. U svrhu zaštite privatnosti učenika i djelatnika škola preporučuje upotrebu zatvorenih privatnih profila na društvenim mrežama, a da pri tom ne prihvaćaju učenika kao prijatelja.

Korisnici su odgovorni za sve neželjene posljedice upotrebe interneta.

Učenici i djelatnici educirat će se o odgovornoj upotrebi interneta u okviru aktivnosti predviđenih školskim kurikulumom, odnosno pohađat će edukacije stručnog usavršavanja.

Svi korisnici, ovisno o težini povrede, odgovaraju za internetsko nasilje koje su počinili. Škola može učenicima izreći pedagošku mjeru u skladu s propisima koji uređuju izricanje pedagoških mjera, a djelatnicima upozorenje na obveze iz radnog odnosa u skladu s propisima radnog prava.

U slučaju saznanja za događaje internetskog nasilja počinjenih prema učenicima, škola je dužna poduzeti potrebne korake i obavijestiti nadležne institucije u skladu s posebnim propisima.

Korištenje mobilnih telefona

Članak 35.

Kućnim redom Škole zabranjeno je korištenje mobilnih telefona za vrijeme nastave.

Iznimno, učenici mogu koristiti mobilne telefone za vrijeme nastave, kada nastavnik to zatraži i pravovremeno najavi.

Učenici mogu u Školi koristiti mobilne telefone za vrijeme odmora, prije ili poslije nastave, poštujući odredbe Kućnog reda Škole i ovog Pravilnika.

S obzirom da mobilni telefoni sve više imaju potpuni pristup internetu te da djeca i mladi koriste fiksne internetske veze kao i mobitele za pretraživanje 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 učenike s posljedicama zlouporabe mobilnih telefona. Najrašireniji oblik nasilja među vršnjacima je nasilje putem mobilnih telefona.

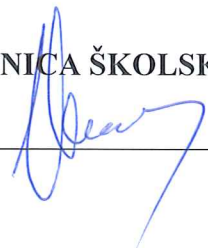
Ono uključuje bilo kakav oblik poruke zbog koje se osoba osjeća neugodno ili joj se tako prijeti (tekstualna poruka, videoporuka, fotografija, poziv), odnosno kojoj je cilj uvrijediti, zaprijetiti, nanijeti bilo kakvu štetu vlasniku mobilnog telefona.

Članak 36.

Ovaj Pravilnik stupa na snagu danom donošenja.

KLASA: 602-03/20-05/13
URBROJ: 251-87-05-20-1
Zagreb, 03. 06. 2020. godine

PREDSJEDNICA ŠKOLSKOG ODBORA:



RAVNIateljica:



Jadranka Pejić, prof.