

Na temelju Članka 29. Statuta OŠ Dragutina Kušlana, (KLASA: 602-02/01-15-22 URBROJ: 251-163-15-01-3 u Zagrebu, 29.6.2015.) , te čl. 118. st. 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 i 7/17) Školski odbor OŠ Dragutina Kušlana na sjednici održanoj 6.srpnja 2018. donosi

## **PRAVILNIK O SIGURNOJ I ODGOVORNOJ UPOTREBI INFORMACIJSKO-KOMUNIKACIJSKE TEHNOLOGIJE OŠ DRAGUTINA KUŠLANA, ZAGREB**

### **I. UVOD**

#### **Članak 1.**

S obzirom na sve veću sustavnu uporabu 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 potrebno posvetiti vidu sigurnog i odgovornog korištenja IKT-a, što je moguće postići definiranjem sigurnosne politike škole.

Pravilnik o sigurnoj i odgovornoj upotrebi informacijsko-komunikacijske tehnologije (dalje u tekstu: Pravilnik) vrijedi za sve korisnike IKT infrastrukture OŠ Dragutina Kušlana (dalje u tekstu: Škola). U Školi je u kolovozu 2017. godine postavljena infrastruktura CARNetove mreže. Učenici, učitelji i ostali zaposleni moraju se pridržavati uputa koje im daje administrator sustava (e-Škole tehničar).

E-škole tehničarem Škole imenovana je učiteljica informatike Ivana Marjanović.

#### **Članak 2.**

Svrha ovog Pravilnika je:

- unaprjeđenje sigurnosti školske informatičke opreme i mreže.
- jasno i nedvosmisленo određivanje načina prihvatljivog i dopuštenog korištenja IKT resursa škole
- zaštita informacijskog sadržaja i opreme
- zaštita korisnika od različitih vrsta internetskog zlostavljanja
- promoviranje sustava i usluga koji su najprikladniji za učenike

- poticanje aktivnog sudjelovanja učenika u radu s IKT-om promovirajući sigurno, odgovorno i učinkovito korištenje digitalnih tehnologija u mrežnoj zajednici, pravilne raspodjele zadatke i odgovornosti nadležnih osoba
- propisivanje sankcija u slučaju kršenja odredbi Pravilnik.

## II. OSNOVNE SIGURNOSNE ODREDBE

### Članak 3.

Kompletna računalna mreža i računalna oprema dobivena u sklopu pilot projekta e-Škola , stara računalna mreža i računalna oprema smatra se IKT infrastrukturom Škole.

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

Materijalni resursi su:

- Kompletna računalna mreža izgrađena u sklopu pilot projekta e-Škole i računalna oprema, stara računalna mreža i računalna oprema smatraju se IKT infrastrukturom.

Nematerijalni resursi su:

- Aplikacije koje škole koristi: e-Dnevnik, e-Matica, HUSO admin, Meraki (središnji sustav za upravljanje računalnom mrežom), Office 365 skup programa, registar zaposlenih u javnom sektoru i aplikacije vezane za finansijsko poslovanje škole i obračun plaća i ostale aplikacije.

### Članak 4.

Školska oprema mora se čuvati i pažljivo koristiti.

### Članak 5.

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

Povjerljive informacije su osobni podatci zaposlenika, učenika (npr. kontakt podatci osobe, fotografije osobe i sl.), podatci iz evidencija koje Škola vodi (e-Dnevnik, e-Matica, matične knjige i dr.), te informacije koje se smatraju poslovnom tajnom. Osobni podatci mogu se koristiti isključivo uz prethodno odobrenje ravnatelja ili osobe koju on za to posebno ovlasti.

## Članak 6.

U Školi sva računala koja rade u Windows operativnim sustavima posjeduju vatrozid, ali ne i antivirusni program (odnosi se na Windows 7, Windows 8 i Windows XP). Noviji operativni sustavi, poput Windows 10, posjeduju Windows Defender Security Center. Učenici, učitelji i ostali zaposleni koji se spajaju na računalnu mrežu svojim privatnim uređajima nemaju nikakvu zaštitu.

Većina mjera zaštite su implementirana kod davatelja internetskih usluga (ISP-a - CARNet). Njihovi serveri blokiraju sadržaje i stанице sumnjivog karaktera. U mrežnom sustavu je blokiran pristup P2P (peer to peer) mrežnom servisu za razmjenu podataka te web stranicama koji podržavaju P2P razmjenu podataka.

## Članak 7.

Svi zaposlenici Škole posjeduju AAI@edu.hr korisnički račun i dužni su koristiti se e-mailom koji su dobili iz AAI@edu.hr sustava u službenoj komunikaciji s nadležnim tijelima i drugim institucijama iz sustava znanosti i obrazovanja.

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

Svi zaposlenici 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 ovim 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).

## III. ŠKOLSKA IKT OPREMA I ODRŽAVANJE

### Članak 8.

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

Računalni otpad zbrinjava se odvojeno od ostalog otpada, a Škola će takav otpad predati ovlaštenom sakupljaču EE otpada,

### Članak 9.

Računala se bežično spajaju na 20 bežičnih pristupnih točaka. Pristupne točke su smještene u svakoj učionici, kabinetu tjelesne i zdravstvene kulture te u zbornici.

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

- a) eduroam,
- b) eSkole,
- c) guest.

- a) Učitelji i učenici na eduroam mrežu spajaju se svojim privatnim ili školskim uređajima gdje se autentificiraju svojim korisničkim podatcima iz AAI@edu.hr sustava. Na taj način se može identificirati i pratiti njihov promet u računalnoj mreži.
- b) eSkole mreža se koristiti za spajanje uređaja u STEM učionicama gdje se učenici i učitelji (samo u slučaju da koriste isti uređaj) spajaju preko Captive portala koji se aktivira prilikom procesa spajanja.
- c) Guest mreža se koristi za spajanje vanjskih partnera i posjetitelja. Partnerima i posjetiteljima koji imaju AAI@edu.hr račun je omogućen pristup na eduroam mrežu uz ograničenje brzine pristupa. Ostalim partnerima i posjetiteljima na zahtjev se može 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.

### Članak 10.

Određena računala u školi spojena su žičanim načinom spajanja na mrežu. U većinu su učionica dovedeni UTP kablovi te se računala mogu spojiti. Računala koja su spojena na taj način spojena su na staru mrežnu infrastrukturu.

Sva računala u informatičkoj učionici (16 + 1), računala u uredima (ured ravnatelja, tajništvo, računovodstvo, zbornica, ured defektologinje i pedagoginje) i knjižnici žičano su spojena. Na računalnu mrežu žičanim putem sveukupno su spojena 23 računala. Računalna

mreža je konfigurirana tako da nema potrebe da se računala/korisnici autentificiraju kada se spajaju u žičanu računalnu mrežu.

### Članak 11.

Većina računala u školi posjeduje operativni sustav Windows 7 s instaliranim Office alatima. Računala u informatičkoj učionici posjeduju Windows 10 s instaliranim Office alatima. Postavke na računalima su podešene na općenite te je na svim računalima postavljeno da nema zaporke kod prijave u operativni sustav (za administratorsku prijavu postavljena je lozinka). Uključena je opcija da lozinka nikada ne ističe (Password never expires). Kod svih računala automatski je podešeno ažuriranje operativnog sustava i popratnih Office alata. Računalna mreža pokazuje da najviše prometa koja računala ostvaruju preko interneta odlazi na ažuriranje navedenog. Operativni sustavi Windows 10 imaju u sebi antivirusni sustav (Windows Defender Security Center) te i vatrozid koji posjeduju i stariji operativni sustavi. Antivirusni programi ako se koriste, koriste se na starijim operativnim sustavima i to besplatne inačice antivirusnih programa (AVG Free). Od filtriranja sadržaja trenutno se filtriraju web stranice koje promoviraju i sadrže P2P (peer to peer) datoteke. Računalna mreža u potpunosti blokira promet P2P.

### Članak 12.

U Školi nema potrebe samostalnog nadziranja licenciranih programa jer su svi programi koji se koriste (Windows XP, 7, 8, 10, Office 2007, 2010, 2013, 2016) 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 resursa, e-tehničari). U sustav se prijavljuje AAI@edu.hr korisničkim računom gdje se mogu preuzeti svi navedeni operativni sustavi i Office alati s pripadajućim ključevima za aktivaciju.

### Članak 13.

Na računala u školi učenici ne smiju ništa instalirati bez odobrenja administratora. Ako se pojavi potreba za instaliranje dodatnog programa učitelj/učenik prethodno obvezno se mora javiti administratoru.

### Članak 14.

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

## IV. REGULIRANJE PRISTUPA IKT OPREMI

### Članak 15.

Računalnoj mreži smiju pristupiti učenici, učitelji, ostali zaposlenici škole te vanjski partneri i posjetitelji.

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

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

- a) eduroam,
- b) eSkole,
- c) guest.

- a) Na eduroam mrežu se spajaju učitelji i učenici sa svojim privatnim ili školskim uređajima gdje se autentificiraju svojim korisničkim podatcima iz AAI@Edu.hr sustava (802.1x with custom RADIUS enkripcija). Na taj način može se identificirati i pratiti njihov promet u računalnoj mreži.
- b) eSkole mreža može se koristiti za spajanje uređaja u STEM učionicama gdje se učenici i učitelji (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).
- c) Guest mreža koristi se za spajanje vanjskih partnera i posjetitelja (Open-password-protected with Meraki RADIUS enkripcija). Partnerima i posjetiteljima koji imaju AAI@edu.hr račun omogućen je pristup na eduroam mrežu uz ograničenje brzine pristupa. Ostalim partnerima i posjetiteljima može se na zahtjev omogućiti pristup bežičnoj mreži. Bežična mreža guest je otvorenog tipa, a za autentifikaciju 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.

### Članak 16.

Svi učitelji dobili su računalo u sklopu projekta e-Škole. Učitelji iz STEM područja dobili su hibridno računalo Lenovo ThinkPad Yoga 260, ravnatelj i stručni suradnici dobili su HP ProBook 640 G2 prijenosno računalo, a ostali učitelji tablet računalo HP 10 EE Z3735F.

### Članak 17.

STEM učionica (učionica biologije, kemije i fizike – br. 20) opremljena je računalima (tabletima) koja učenici mogu koristiti samo uz odobrenje učitelja. Učitelji i ostali zaposleni imaju pristup računalima jedno stolno i jedno prijenosno računalo) koja su smještena u zbornici. Učitelji ne moraju tražiti posebno odobrenje za korištenje informatičke učionice.

### Članak 18.

Učenici smiju koristiti računala samo uz dopuštenje i nadzor učitelja. U STEM učionicama učenici se smiju koristiti računalnom opremom samo uz odobrenje učitelja. Pristup aplikacijama i internetskim sadržajima isključivo određuje učitelj.

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

### Članak 19.

Svi učitelji koji koriste informatičku učionicu moraju se držati sljedećeg:

- učionica mora ostati na kraju u stanju u kojem je i zatečena
- računala se obavezno moraju ugasiti nakon zadnjeg nastavnog sata u informatičkoj učionici tog radnog dana
- u slučaju da jedno od računala ne radi – obvezno je kontaktirati i o tome obavijestiti učitelja informatike
- radno mjesto u učionici mora ostati uredno – namještена tipkovnica, miš, monitor, stolica moraju biti postavljeni na svojem mjestu
- učionica se nakon korištenja zaključava.

Učitelj koji koristi informatičku učionicu odgovoran je za stanje u učionici.

### Članak 20.

Za ulaz učenika u operativni sustav ne koristi se zaporka i to je račun bez administratorskih ovlasti. Učitelji imaju račun administratora s postavljenom lozinkom koja je poznata učiteljima. U operativnom sustavu uključena je opcija da lozinka nikada ne prestaje (Password never expires).

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. U mrežnom sustavu Škole dodatno je uključeno blokiranje pristupa P2P (peer to peer) mrežnom servisu za razmjenu podataka, te web stranicama koji podržavaju P2P razmjenu podataka.

Škola je dužna sve učenike škole upoznati s informacijama o sustavu, odnosno da je sustav podešen tako da filtrira nepoćudan sadržaj i to im posebno naglasiti, te ih o tome dodatno educirati i uputiti na nastavi informatike. Učenici su stalno pod nadzorom i u potpunosti im je onemogućeno zaobilaženje sigurnosnih postavki računalne opreme.

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

#### **IV. SIGURNOST KORISNIKA**

##### **Članak 21.**

Škola u suradnji s vanjskim suradnicima sustavno provodi edukaciju učenika, učitelja i ostalih zaposlenika kako bi se mogao održati korak u korištenju IKT-a, kao i s nadolazećim prijetnjama u računalnoj sigurnosti.

Svi učitelji i ostali zaposlenici pri korištenju računala i programa koji zahtijevaju prijavu posebno moraju voditi računa da pri prijavi ne otkriju svoje podatke za prijavu. 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.

##### **Članak 22.**

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

U potpunosti je omogućeno preuzimanje datoteka na lokalna računala te pokretanje izvršnih datoteka. Ako se pokaže da se na taj način računala inficiraju zlonamjernim programima, e-tehničar može uvesti restrikciju na takvu vrstu interakcije.

Svi učenici, učitelji i ostali zaposleni posjeduju Elektronički identitet u sustavu AAI@Edu.hr. Škola po potrebi ustrojava evidenciju korisničkih računa. Svi učenici dobivaju elektronički identitet ispisan u analognom obliku koji im se daje na čuvanje i korištenje. U slučaju gubitka korisničkog računa, učenik ili roditelj dolazi u tajništvo škole i tajnik škole (administrator imenika) ispisuje korisnički račun s novom lozinkom. U slučaju preseljenja učenika u drugu školu, njegov se elektronički identitet privremeno briše. U slučaju dolaska učenika iz druge škole njegov se elektronički identitet prenosi. Isto vrijedi i za učitelje i ostale zaposlene.

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

Odlaskom u mirovinu ili prestankom rada u školskom ustavu, učiteljima i ostalim zaposlenima prestaju prava nad korisničkim identitetom.

## **V. PRIHVATLJIVO I ODGOVORNO KORIŠTENJE IKT-a**

### **Ponašanje na internetu**

#### **Članak 23.**

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.

Svaki korisnik koji se susreće s internetom dužan je upoznati se s osnovnim pravilima poželjnog ponašanja u takvoj komunikaciji i takvom okruženju, odnosno dužan je koristiti se tzv. 'internetskim bontonom' ili 'Netiquette'. 'Netiquette', ustaljen popis pravila lijepog ponašanja u internetskoj komunikaciji na hrvatskom jeziku dostupan je na <http://hr-netiquette.org>.

Škola je „internetski bonton“ učinila dostupnim svojim učenicima, o tome ih podučava, te primjenjuje vlastitu politiku u skladu s tim pravilima.

#### **Članak 24.**

Učenike se na nastavi informatike i na satu razrednog odjela poučava osnovnim pravilima ponašanju 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 25.

Osim Internetskog bontona 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 odgovarati na zlonamjerne ili prijeteće poruke!
- Treba pomoći prijateljima koji su zlostavljeni preko interneta tako da se to ne prikriva i da se odmah obavijeste odrasli.
- Potrebno je biti oprezan s izborom fotografija koje se objavljaju na društvenim mrežama.
- Treba provjeriti postoji li neka mrežna stranica o nama te koje informacije sadrži (treba upisati svoje ime i prezime u Google).

### Autorsko pravo

### Članak 26.

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

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

Računalni programi također su 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 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.

## VI. DIJELJENJE DATOTEKA

### Članak 27.

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

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 torrenta. Torrent klijenti će se moći instalirati i pokrenuti, ali neće moći ostvariti nikakav mrežni promet.

Obveza Škole je:

- 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 učitelja podučiti o načinima nelegalnog dijeljenja datoteka i servisima koji to omogućuju poput Torrent servisa, mrežnog mesta 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.

## VII. INTERNETSKO NASILJE

### Članak 28.

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.

U školi je nedopušten bilo koji oblik nasilničkog ponašanja te takvo ponašanje za posljedicu može imati izricanje pedagoških mjera.

### Članak 29.

Škola redovito provodi edukaciju o neprihvatljivom ponašanju kroz predmete koji koriste tehnologiju ili sat razrednika, a pravila o prihvatljivom ponašanju i korištenju tehnologije vidljiva su 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 o njima podučiti učenike 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

## VIII. KORIŠTENJE MOBILNIH TELEFONA

### Članak 30.

Kućnim redom škole propisano je da je zabranjeno korištenje mobilnih uređaja za vrijeme nastave. U suprotnom učitelj ima pravo učeniku oduzeti mobitel i pohraniti ga kod sebe, u tajništvo ili kod ravnatelja škole. Mobitel može preuzeti isključivo učenikov roditelj ili skrbnik.

Sukladno odluci Učiteljskog vijeća i odredbama Kućnog reda učenici ne mogu koristiti mobitel ni u slobodno vrijeme (mali i veliki odmor).

Iznimno, učenici mogu koristiti mobitele (smartphone) ili druge mobilne uređaje i za vrijeme nastave kao nastavno pomagalo kada učitelj to zatraži i pravovremeno najavi. Svaka upotreba tehnologije u učionici mora imati unaprijed zadani 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 najraširenijih oblika nasilja među vršnjacima je nasilje putem mobitela. Nasilje putem mobitela uključuje bilo kakav oblik poruke zbog koje se osoba osjeća neugodno ili joj se tako prijeti. Ta poruka može biti tekstualna, video poruka, 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.

### Članak 31.

Vezano uz sigurnu upotrebu mobilnih telefona koji imaju potpuni pristup internetu, na isti način kao i kod primjene ostale IKT tehnologije, što se posebno odnosi na primjenu Pravila poželjnog ponašanja, tzv. Internetski bonton i Pravila sigurnog ponašanja.

### ZAVRŠNE ODREDBE

### Članak 32.

Ovaj Pravilnik stupa na snagu danom njegovog donošenja.

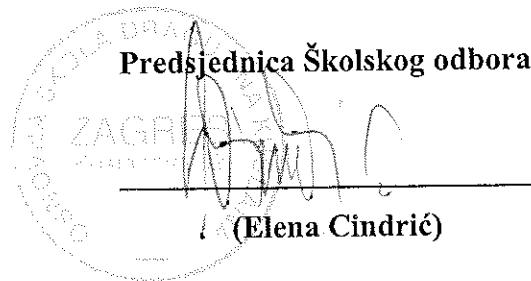
Sve izmjene i dopune ovog Pravilnika donose se u istom postupku i na isti način kao i ovaj Pravilnik.

Sukladno Zakonu o pravu na pristup informacijama, ovaj Pravilnik bit će objavljen na internetskoj stranici Naručitelja.

KLASA: 003 - 06/18 - 01/12  
URBROJ: 251-163-18-01-3

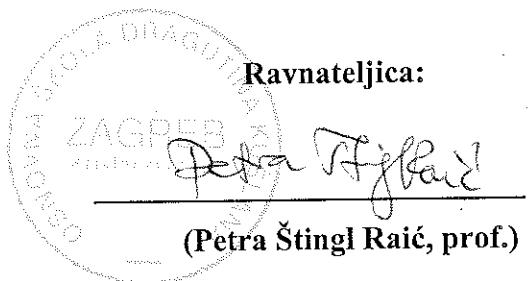
Zagreb, srpanj 2018.

Predsjednica Školskog odbora:



Ovaj Pravilnik objavljen je na internetskoj stranici OŠ Dragutina Kušlana [http://os-kuslana-zg.skole.hr/dokumenti/va\\_ni\\_dokumenti](http://os-kuslana-zg.skole.hr/dokumenti/va_ni_dokumenti).

Ravnateljica:



(Petra Štingl Raić, prof.)