OŠ Šećerana, Šećerana

Žrtava Domovinskog rata 27

31300 Beli Manastir

**PRAVILNIK**

**O SIGURNOJ I ODGOVORNOJ UPOTREBI INFORMACIJSKO-KOMUNIKACIJSKE TEHNOLOGIJE U**

**OSNOVNOJ ŠKOLI ŠEĆERANA**

U Šećerani, 31. svibnja 2023. Na temelju članka 51. Statuta Osnovne škole Šećerana Školski odbor na sjednici održanoj 31. svibnja 2023. godine donosi

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

# Uvod

Članak 1.

Svrha Pravilnika o sigurnoj i odgovornoj upotrebi informacijsko-komunikacijske tehnologije (u daljnjem tekstu: Pravilnika) je određivanje načina prihvatljivog i dopuštenog korištenja IKT resursa Škole.

Pravilnik vrijedi za sve korisnike IKT infrastrukture Škole – učenike, učitelje, stručne suradnike, administrativno i tehničko osoblje te goste.

 U školi je postavljena CARNetova mreža.

Svi korisnici trebaju se pridržavati uputa koje im daje administrator sustava i e-Škole tehničar.

Učenici se moraju pridržavati uputa koje im mogu dati učitelji, a kojima je cilj unaprjeđivanje sigurnosti školske informatičke opreme i mreže.

Učitelji i drugi korisnici IKT opreme moraju se pridržavati uputa koje im može dati školski administrator sustava ili neka druga ovlaštena osoba radi unaprjeđivanja sigurnosti školske informatičke opreme i mreže.

# Osnovne sigurnosne odredbe

Članak 2.

Materijalni i nematerijalni resursi su:

* Korisnici IKT infrastrukture su učenici, učitelji, ostali djelatnici škole i povremeni korisnici (gosti).
* Kompletna računalna mreža izgrađena u sklopu pilot projekta e-Škole i računalna oprema smatraju se IKT infrastrukturom.
* Aplikacije koje škola koristi: e-Matica, Carnet id, e-Dnevnik, Riznica za financijsko poslovanje, MetelWin program za školsku knjižnicu, Office 365.

Školska oprema se mora čuvati i pažljivo koristiti.

Članak 3.

S obzirom na dostupnost financija sigurnosne mjere zaštite podataka su na prosječno zadovoljavajućoj razini. Trenutno na računalima na kojima je instaliran Windows operacijski sustav (Windows 8) za zaštitu od virusa, zlonamjernih programa, špijunskog i ostalog zlonamjernog softvera u stvarnom vremenu koristimo paket pod nazivom Microsoft Security Essentials i aktiviran vatrozid. Noviji operacijski sustavi, poput Windows 8.1 , 10 i 11 , posjeduju ugrađen program za zaštitu od virusa i zlonamjernih programa pod nazivom Windows Defender Security Center.

Učenici, učitelji i ostali djelatnici koji se spajaju na računalnu mrežu sa svojim privatnim pametnim telefonima čiji su sustavi android, ios, windows operacijski sustav, nemaju nikakvu zaštitu.

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

Svi zaposlenici naše škole posjeduju AAI@EduHr korisnički račun pa su tako dužni koristiti e- mail koji su dobili iz AAI@EduHr sustava u službenoj komunikaciji s nadležnim tijelima i drugim institucijama iz sustava znanosti i obrazovanja.

Učiteljima i drugim djelatnicima je strogo zabranjeno davati učenicima i drugim korisnicima vlastite zaporke, zaporke mreže i druge digitalne identitete školskog mrežnog sustava.

Svi djelatnici škole, učenici i gosti moraju se pridržavati etičkih načela pri korištenju IKT-a.

Svako nepridržavanje pravila od strane zaposlenika, učenika ili gosta škole 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 .

# Školska IKT oprema i održavanje

Članak 4.

Računala u školi su povezana bežično i žičano. Računalna mreža izgrađena je u sklopu pilot projekta e-Škole.

Računalni otpad odvozi ovlaštena tvrtka Metal Zec d.o.o..

Računala u matičnoj školi se bežično spajaju na 21 bežičnu pristupnu točku. U PŠ Baranjsko Petrovo Selo ima 20 pristupnih točaka, PŠ Branjin Vrh na 9 pristupnih točaka, PŠ Luč na 3 pristupne točke, PŠ Petlovac je na 1 pristupnoj točci i PŠ Torjanci na 3 pristupne točake. Pristupne točke su smještene u učionicama i u prostorima škole (zbornica, hol, dvorana, knjižnica).

Spajanje na mrežu omogućeno je preko:

* eduroam,
* eSkole,
* guest
* otvorenamreza.org.

 Na eduroam mrežu se spajaju učitelji i učenici sa svojim privatnim ili školskim uređajima gdje se prijavljuju svojim korisničkim podatcima iz AAI@EduHr sustava. Na taj način se može pratiti njihov rad u računalnoj mreži.

 eSkole mreža se koristiti za spajanje tablet uređaja za učenike (164 tableta u matičnoj i područnim školama) u svim učionicama u kojima učenici koriste tablete.

 Guest mreža se koristi za spajanje vanjskih partnera i posjetitelja. Partnerima i posjetiteljima koji imaju AAI@edu račun je omogućen pristup na eduroam mrežu uz ograničenje brzine pristupa. Ostalim partnerima i posjetiteljima se može na zahtjev omogućiti pristup bežičnoj mreži.

 Otvorena mreža dostupna je svim korisnicima u Školi i izvan nje u krugu od 20 metara oko škole.

Računala koja su spojena žičano su sva računala u informatičkoj učionici u matičnoj školi (16 računala), PŠ Baranjsko Petrovo Selo ( 9 računala), PŠ Branjin Vrh (5 računala), računala u učionicama i računala u uredima (ured ravnateljice, tajništvo, računovodstvo, zbornica, ured pedagoga, knjižnica). Sveukupno 10 računalo je spojeno na računalnu mrežu žičanim putem.

Većina računala u školi posjeduje operacijski sustav Windows 11 s instaliranim Office 2016 alatima. Nekoliko starijih računala i sva računala u informatičkoj učionici posjeduju Windows 8 operacijski sustav s instaliranim Office 2013 alatima. Postavke na računalima u informatičkoj učionici postavljene su na općenite te na dijelu starijih računala postoji zaporka. Ostala računalima nema zaporke kod prijave u sustav. Također je uključena opcija da lozinka nikada ne ističe (Password never expires). Kod svih računala je postavljeno ažuriranje operacijskog sustava i popratnih office alata na automatski. Računalna mreža pokazuje da najviše prometa koja računala ostvaruju preko interneta odlazi na ažuriranje navedenog. Operacijski sustavi Windows 8 i Windows 10 imaju u sebi obrambeni sustav (Windows Defender Security Center) te također i vatrozid koji posjeduju i stariji operativni sustavi do Winodwsa7. Od filtriranja sadržaja trenutno se filtriraju web stranice koje promoviraju i sadrže P2P (peer to peer) datoteke. Računalna mreža u potpunosti blokira promet P2P.

Trenutno u školi nema potrebe samostalnog nadziranja licenciranih programa jer svi programi koji se koriste (Windows 7, 8.1, 10, 11, Office 2013, 2016, 2018) su licencirani od strane Ministarstva znanosti i obrazovanja i tvrtke Microsoft. Ministarstvo znanosti i obrazovanja je izradilo web portal Centar za preuzimanje Microsoft proizvoda. Pristup portalu imaju svi odgovorni za održavanje i instalaciju računalnih programa u školama (administratori sustava, e-tehničari ). U sustav se prijavljuje AAI@edu korisničkim računom gdje se mogu preuzeti svi navedeni operacijski sustavi i office alati s pripadajućim ključevima za aktivaciju.

Učenici ne smiju instalirati dodatne računalne programe u informatičkoj učionici na računala učenika (igrice ili nekakav drugi program), niti deinstalirati programe instalirane na računalo .

Svako nepridržavanje ovih pravila ima negativan utjecaj po Školu i može rezultirati izricanjem pedagoških mjera učenicima sukladno Pravilniku o kriterijima za izricanje pedagoških mjera.

# Reguliranje pristupa IKT opremi

Članak 5.

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

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

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

1. eduroam,
2. eSkole,
3. guest
4. otvorena mreža.
5. Na eduroam mrežu se spajaju učitelji i učenici sa svojim privatnim ili školskim uređajima gdje se autentificiraju svojim korisničkim podacima iz AAI@EduHr sustava (802.1x with custom RADIUS enkripcija). Na taj način se može identificirati i pratiti njihov promet u računalnoj mreži.
6. eSkole mreža se koristi 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).
7. Guest mreža se koristi za spajanje vanjskih partnera i posjetitelja (Open-password- protected with Meraki RADIUS enkripcija). Partnerima i posjetiteljima koji imaju AAI@edu račun je omogućen pristup na eduroam mrežu uz ograničenje brzine pristupa. Ostalim partnerima i posjetiteljima se može na zahtjev omogućiti pristup bežičnoj mreži. Bežična mreža guest je otvorenog tipa, a za autentikaciju se koristi tzv. captive portal. Kako bi im se omogućio pristup, e-Škole tehničar u Meraki dashboardu mora kreirati korisničko ime za svakog korisnika kojem škola odobri pristup mreži.
8. Otvorenoj mreži dozvoljen je pristup svim korisnicima neograničeno.

U okviru projekta e-Škole učitelji iz STEM područja su računalo HP Probook 455G6R ( 26 komada) i HP Probook 455 G7 ( 17 komada), dakle ukupno 43 laptopa.

# STEM učionice

Članak 6.

STEM učionice (učionice biologije/kemije/fizike i matematike) su opremljene tabletima koji učenici mogu koristiti samo uz odobrenje nastavnika. Nastavnici i ostalo osoblje također imaju pristup računalima koji je smješteni u zbornici te informatičkoj učionici. Učitelji bi u pravilu trebali zatražiti posebno odobrenje za korištenje informatičke učionice kako bi im učitelj informatike pripremio učionicu te instalirao na računala potrebne programe za rad.

Kod prvog korištenja obavezno upoznati učenike s pravilima ponašanja tijekom korištenja tableta. (Gdje se pale, gdje se gase, kako ih držimo na stolu, kako pretražujemo, po koracima što od njih očekujete da rade, higijena ruku, brisanje na dva kvadratića svega što je otvarano, brisanje ekrana nakon korištenja.

Učitelj provjerava je li sve odjavljeno i vraća tablete te ih spaja na punjenje i zaključava ormar.

Učenici smiju koristiti računala i tablete samo uz dopuštenje učitelja.

U informatičkoj učionici strogo je zabranjeno konzumiranje hrane i pića. Zabranjeno je trčanje, vijanje i naguravanje kako ne bi došlo do oštećivanja računala i ostale računalne opreme. Svaku štetu koju učenik napravi u informatičkoj učionici dužan je nadoknaditi.

Svako oštećenje ili kvar koji učenik uoči u informatičkoj učionici učenik je dužan prijaviti učitelju informatike ili učitelju koji trenutačno boravi i radi u informatičkoj učionici.

U informatičkoj učionici učenici se trebaju držati higijenskog protokola prilikom pristupanja računalu ( pranje ruku prilikom pristupanja računalu, pranje ruku nakon školske užine i sl.)

Na nastavi informatike učenici ako su prethodno dobili odobrenje od nastavnika za uključivanje računala smiju pod odmorom koristiti računalo za potrebe nastave .

Igranje igara za vrijeme održavanje nastave informatike je strogo zabranjeno.

Pristup aplikacijama i internetskim sadržajima određuje isključivo učitelj informatike.

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

Svi učitelji koji koriste informatičku učionicu moraju se držati sljedećeg:

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

Učitelj informatike i svi drugi učitelji koji ulaze u informatičku učionicu su odgovorani za informatičku učionicu i cjelokupnu opremu u informatičkoj učionici.

Članak 7.

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

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

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

# Sigurnost korisnika

Članak 8.

U Školi je potrebno provoditi neprekidnu edukaciju učenika, učitelja i cijelog školskog kolektiva kako bi se mogao održati korak u korištenju IKT-a, kao i s nadolazećim prijetnjama u računalnoj sigurnosti.

 Učitelji i učenici moraju voditi brigu o tajnosti svojih podataka prilikom prijavljivanja i odjavljivanja s uređaja koji koriste.

Isto tako učitelji kada odlaze iz učionice, moraju obavezno isključiti računalo koje su koristili, te se prije isključivanja računala moraju obavezno odjaviti iz svih sustava u koje su se prijavili. Isto vrijedi i za računala koja se nalaze u zbornici.

Ukoliko učenici koriste tablete i računala u STEM i ostalim učionicama obavezno nakon završetka rada moraju se odjaviti iz sustava u koji su se prijavili.

Učenici, učitelji i ostali djelatnici moraju brinuti o svom digitalnom identitetu koji su dobili iz sustava AAI@edu. Svoje podatke moraju čuvati.

Svi učenici, učitelji te ostalo osoblje posjeduje Elektronički identitet u sustavu AAI@Edu.hr. U slučaju gubitka korisničkog računa, učenik ili roditelj dolazi administratoru škole gdje administrator škole ispisuje korisnički račun s novom lozinkom. U slučaju da učenik seli iz naše škole u neku drugu školu, njegov se eketronički identitet privremeno odjavljuje. U slučaju da učenik iz druge škole dolazi u našu školu dobiva elektronički identitet za našu školu. Isto vrijedi i za učitelje i ostalo osoblje.

Članak 9.

Završetkom školovanja učenicima prestaju prava nad elektroničkim identitetom škole koju su polazili.

Učiteljima i ostalom osoblju prestaju prava korištenja elektroničkog identiteta odlaskom u mirovinu ili prestankom rada u školskom sustavu.

# Prihvatljivo i odgovorno korištenje informacijsko-komunikacijske tehnologije

## Ponašanje na internetu

Članak 10.

Svaki pojedinac je odgovoran za svoje ponašanje u virtualnom svijetu te se prema drugim korisnicima mora ponašati pristojno.

Članak 11.

Na satu razrednika razrednici su u obvezi upoznati sve učenike s pravilima ponašanja na internetu koji se nalaze na mrežnoj stranici škole (ne otkrivati osobne podatke, svoju adresu, ime škole, telefonske brojeve i slično preko interneta na npr. Društvenim mrežama, chat sobama...).

Članak 12.

Pravila sigurnog ponašanja:

* Osobne informacije na internetu se nikada ne smiju odavati.
* Zaporka je tajna i nikada se ne smije nikome reći.
* Ne odgovarajte na zlonamjerne ili prijeteće poruke!
* Treba pomoći prijateljima koji su zlostavljani preko interneta neprikrivanjem situacije te odmah obavijestiti učitelja informatike, razrednika, roditelje ili policiju ako postoji intencija na krivično djelo.
* Provjeriti jesu li na profilima društvenih mreža postavljene postavke privatnosti na pravi način.
* Učenici bi trebali biti oprezniji prema ljudima koje primaju za prijatelje.
* Potrebno je biti oprezan s izborom fotografija koje se objavljuju na društvenim mrežama.
* Treba provjeriti postoji li neka mrežna stranica o nama te koje informacije sadrži (*treba upisati svoje ime i prezime u Google*).
* U internetskoj komunikaciji ne koristiti govor mržnje.

## Autorsko pravo

Članak 13.

Autorska prava na online dokumentima najčešće se definiraju s tzv. Creative Commons (CC) licencama (više na <https://creativecommons.org/licenses/?lang=hr>) .

Creative Commons licence jesu skup autorsko-pravnih licenci pravovaljanih u čitavom svijetu. Svaka od licenci pomaže autorima da zadrže svoja autorska prava, a drugima dopuste da umnožavaju, distribuiraju i na neke druge načine koriste njihova djela, barem u nekomercijalne svrhe. Svaka Creative Commons licenca osigurava davateljima licence i da ih se prizna i označi kao autore djela.

Članak 14.

Učitelje, učenike i ostale djelatnike treba poticati na potpisivanje materijala koji su sami izradili koristeći neku licencu te da poštuju tuđe radove.

Nipošto ne smije tuđe radove predstavljati kao svoje, preuzimati zasluge za 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 mrežni programi odnosno 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.

## Dijeljenje datoteka

Članak 15.

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

Članak 16.

Primjer nelegalnog dijeljenja datoteke jeste kopiranje ili preuzimanje autorski zaštićenog materijala poput e-knjige, glazbe ili pak audio i 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, 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.

Na računala je također strogo zabranjeno instaliranje nelegalnih programa s lažnim ključevima licence ( piratskim programi).

Članak 17.

**Obveze ustanove su:**

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

## Internetsko nasilje

Članak 18.

Internetsko nasilje se općenito može definirati kao namjerno i opetovano nanošenje štete korištenjem računala, mobitela i drugih elektroničkih uređaja. Nasilje preko interneta, u svijetu poznato kao cyberbullying, opći je pojam za svaku komunikacijsku aktivnost cyber tehnologijom koja se može smatrati štetnom kako za pojedinca, tako i za opće dobro.

Postoje različiti oblici internetskog nasilja:

* nastavljanja slanja e-pošte usprkos tome što netko više ne želi komunicirati s pošiljateljem
* lažno predstavljanje žrtve na internetu
* slanje prijetećih poruka žrtvi koristeći različite internetske servise (poput društvenih mreža, Skypea, e-maila i drugih servisa za komunikaciju)
* postavljanje internetske ankete o žrtvi
* stvaranje grupa na drušvenim mrežama tipa “svi mi koji mrzimo xy”
* govor mržnje (diskriminacija po spolu, rasi, nacionalnosti, vjeri, fizičkom izgledu i sl.)
* slanje virusa na e-mail ili mobitel
* slanje uznemirujućih fotografija putem e-maila, mms-a ili drugih komunikacijskih alata.

Nasilje u školama je postao sve veći problem tijekom nekoliko posljednjih godina, a budući da sve više djece koristi internet i mobilne telefone za komuniciranje.

Iako se velika većina incidenata može riješiti neformalnim putem (zvanjem roditelja, slanjem djece na razgovor stručnoj službi Škole i sl.), postoje i situacije kad se zahtijeva službena reakcija škole. To se događa u slučajevima koji uključuju ozbiljne prijetnje prema drugim učenicima, a rezultiraju time da žrtva više ne želi ići u školu ili pak ako se nasilje nastavi iako su već korištena druga neformalna sredstva.

Svi oblici nasilničkog ponašanja u školi su nedopušteni i disciplinski će odgovarati svi oni za koje se utvrdi da provode takve aktivnosti. Teži slučajevi elektroničkog nasilja i govora mržnje bit će prijavljeni policiji.

Edukacija o neprihvatljivom ponašanju provodi se kroz nastavu informatike, predmete koji koriste IT tehnologiju ili Sat razrednika. Pravila o prihvatljivom ponašanju i korištenju tehnologije vidljiva i u prostorijama škole.

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

Škola se obvezuje da će:

1. Poučiti učenike, učitelje i roditelje na roditeljskim sastancima o mogućim oblicima internetskog nasilja i govora mržnje.
2. Učenike, učitelje i roditelje poučiti o tome kako prepoznati internetsko nasilje.
3. Jasno istaknuti prihvatljiva pravila ponašanja za učenike i učitelje koji u radu

 koriste IT tehnologiju.

1. Izraditi strategiju odgovora na internetsko nasilje, bilo da je u pitanju blaži i teži oblik elektroničkog nasilja i govora mržnje.
2. Razviti nultu stopu tolerancije na internetsko nasilje.
3. Obilježavati Dane sigurnijeg interneta i suzbijanja nasilja kroz radionice, diskusije i kreativne radove.

## Korištenje mobilnih telefona – određeno čl. 16 Kućnog reda Škole

Članak 19.

Učenici su dužni za vrijeme boravka u Školi isključiti zvuk mobitela. Zabranjuje se bilo kakvo korištenje mobitela (telefoniranje, SMS, mobilni internet, slušanje glazbe, fotografiranje i sl.) tijekom nastave osim ako je to predviđeno planiranim nastavnim satom.

Strogo je zabranjeno snimanje učitelja, učenika i drugih djelatnika Škole tijekom nastave, te objavljivanje video, foto ili audio snimaka na društvenim mrežama, te dijeljenje video, foto ili audio snimaka putem e-maila ili drugih oblika dijeljenja gore navedenih datoteka.

Učenik smije koristiti mobitel tijekom odmora.

Učeniku koji koristi mobitel protivno odredbama ovoga članka, predmetni nastavnik ili dežurni učitelj smije privremeno oduzeti mobitel i vratiti ga učeniku ili roditelju/skrbniku na kraju nastavnog sata ili dana.

Sigurnosne mjere za korištenje interneta postaju važeće i za korištenje mobilnih telefona (zaštita osobnih podataka, izbjegavanje štetnih sadržaja, zaštita potrošača, ovisnost o računalnim igrama, i slično).

Ovaj Pravilnik stupa na snagu danom donošenja.

 Predsjednica školskog odbora: