



OSJEČKO-BARANJSKA ŽUPANIJA
OSNOVNA ŠKOLA
SILVIJE STRAHIMIR KRANJČEVIĆ
LEVANJSKA VAROŠ, GLAVNA 62
OIB: 84240970996

**PRAVILNIK
O SIGURNOJ I ODGOVORNOJ UPOTREBI
INFORMACIJSKO-KOMUNIKACIJSKE TEHNOLOGIJE U
OSNOVNOJ ŠKOLI „SILVIJE STRAHIMIR KRANJČEVIĆ“**

U Levanjskoj Varoši, 31. svibnja 2023.

Na temelju članka 47. Statuta Osnovne škole „Silvije Strahimir Kranjčević“
Školski odbor na sjednici održanoj 31. svibnja 2023.. godine donosi

PRAVILNIK O SIGURNOJ I ODGOVORNOJ UPOTREBI INFORMACIJSKO-KOMUNIKACIJSKE TEHNOLOGIJE U OSNOVNOJ ŠKOLI „SILVIJE STRAHIMIR KRANJČEVIĆ“

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 lipnju 2022. godine u školi je postavljena CARNetova mreža.

Svi korisnici trebaju se pridržavati uputa koje im daje administrator sustava i e-Škole tehničar. Administrator sustava za OŠ „Silvije Strahimir Kranjčević“ je učitelj informatike Hrvoje Šen, a e-Škole tehničara, Branko Mandarić, imenovao je osnivač Osječko-baranjska županija.

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, nastavnici, ostali djelatnici i povremeni korisnici (gosti).
- Kompletna računalna mreža izgrađena u sklopu projekta CARNeta i računalna oprema smatraju se IKT infrastrukturom.
- Aplikacije koje škola koristi: e-Matica, HUSO, e-Dnevnik, Riznica OBZ i COP kao programi za računovodstvo, MetelWin program za školsku knjižnicu, Office 365

Školska oprema se mora čuvati i pažljivo koristiti.

Članak 3.

Tuđi osobni podaci škole mogu se koristiti isključivo samo uz prethodno odobrenje ravnatelja škole.

S obzirom na dostupnost financija sigurnosne mjere zaštite podataka su na prosječno zadovoljavajućoj razini. Trenutno u računalima u kojima je instaliran Windows operativni sustav (Windows 7) za zaštitu od virusa, zlonamjernih programa, špijuskog i ostalog zlonamjernog softvera u stvarnom vremenu koristimo paket pod nazivom ESET Endpoint Antivirus i aktiviran vatrozid. Noviji operativni sustavi, Windows 10, posjeduju ugrađen program za zaštitu od virusa i zlonamjernih programa pod nazivom Windows Defender Security Center. Učenici, nastavnici i ostali djelatnici koji se spajaju na računalnu mrežu sa svojim privatnim pametnim telefonima čiji su sustavi android, Ios, windows operativnim sustavima, 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. Zaposlenici naše škole posjeduju svi 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 i druge digitalne identitete.

Svi djelatnici 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 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 projekta CARNeta.

Računalni otpad odvozi ovlaštena tvrtka MS MOBILE d.o.o..

Računala se bežično spajaju na 22 bežične pristupne točke. Pristupne točke su smještene u učionicama i u prostorima škole (zbornica, hol, dvorana, knjižnica).

Spajanje na mrežu omogućeno je preko:

- eduroam,
- eSkole,
- guest
- otvorena mreza.org.

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

eSkole mreža se koristi za spajanje tablet uređaja za učenike (30 tableta) 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 na području Levanjske Varoši.

Računala koja su spojena žičano su sva računala u informatičkoj učionici (11 računala), računala u učionicama i računala u uredima (ured ravnateljice, tajništvo, računovodstvo, zbornica, ured pedagoga, knjižnica). Sveukupno 21 računalo je spojeno na računalnu mrežu žičanim putem.

Trenutno samo 2 prijenosna i 4 stolna računala posjeduju operacijski sustav Windows 7 i Office 2013 paket alata. Sva ostala računala u školi imaju instaliran operativni sustav Windows 10 s Office 2016 alatima. Postavke na računalima u informatičkoj učionici postavljene su na općenite te na svim 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 operativnog sustava i popratnih Office alata na automatski. Računalna mreža pokazuje da najviše prometa koja računala ostvaruju preko interneta odlazi 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 Windows 7.

Trenutno u školi nema potrebe samostalnog nadziranja licenciranih programa jer svi programi koji se koriste (Windows 7, 10, Office 2013, 2016, 2019) 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 operativni sustavi i office alati s pripadajućim ključevima za aktivaciju. Učenici smiju instalirati dodatne računalne programe u informatičkoj učionici na računala učenika (igre ili nekakav drugi program) na lokalnu D particiju. Na ostala računala u školi učenici ne smiju ništa instalirati bez odobrenja učitelja.

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 tri naziva za pristup bežičnoj mreži (SSID):

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

- a) Na eduroam mrežu se spajaju nastavnici 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.
- b) eSkole mreža se koristi za spajanje uređaja u STEM učionicama gdje se učenici i nastavnici (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 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.

Članak 6.

STEM učionice (učionice biologije/kemije/fizike i matematike) će biti opremljene, a kada budu opremljene tabletima koji učenici mogu koristiti samo uz odobrenje nastavnika. Nastavnici i ostalo osoblje također imaju pristup računalu koje je smješteno u zbornici te informatičkoj učionici. Učitelji ne moraju tražiti posebno odobrenje za korištenje informatičke učionice.

Na Office 365 nalazi se tablica za planiranje korištenja učeničkih tableta.

Ključ od ormara punjača tableta nalaziti će se u uredu ravnateljice i kod domara. Ako koristite opremu u informatičkoj učionici prvo uključite računalo na kućištu zatim ekran na daljinskom upravljaču.

Za pisanje po ekranu osjetljivom na dodir koristimo program Magic IWB ili Paint te pripadajuću olovku.

Za povezivanje s tabletima i ekranom klikni na SORCE na daljinskom upravljaču i izaberi opciju SCREEN MIRRORING.

Ako učionicu koristite posljednji u danu onda prvo gasite na ekranu računalo na isključi, a potom gasite na daljinskom upravljaču ploču.

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 u učionicu matematike tablete te ih spaja na punjenje i zaključava ormar.

Učenici smiju koristiti računala i tablete samo uz dopuštenje nastavnika.

Na nastavi informatike učenici ako su prethodno dobili odobrenje od nastavnika za uključivanje računala smiju pod odmorom koristiti računalo za svoje potrebe. Eventualno na kraju drugog sata (nastava informatike se održava dva sata zaredom) ako su učenici uspješno prošli sve etape nastavnog procesa tada smiju koristiti računalo uz odobrenje nastavnika (za pristup internetskim sadržajima i za zabavu). U STEM učionicama učenici će također smijeti koristiti računalnu opremu samo uz odobrenje nastavnika. Pristup aplikacijama i internetskim sadržajima određuje isključivo nastavnik.

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

Svi učitelji koji koriste informatičku učionicu moraju se držati sljedećeg:

- učionica mora ostati na kraju onako kako je i zatečena
- računala se obavezno moraju ugasi 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

Nastavnik informatike je odgovoran za informatičku učionicu.

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.

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 zaobilazanje 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, a ostavljaju računalo uključeno, obavezno se moraju odjaviti iz svih sustava u koje su se prijavili.

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 u tajništvo škole gdje tajnik škole ispisuje korisnički račun s novom lozinkom. U slučaju da učenik seli iz naše škole u neku drugu školu, njegov elektronički identitet privremeno se briše. U slučaju da učenik iz druge škole dolazi u našu

školu dobiva elektronički identitet za našu školu. Isto vrijedi i za nastavnike 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 (da ne otkrivaju osobne podatke, svoju adresu, ime škole, telefonske brojeve i slično preko interneta na npr. Facebooku, Twiteru, chat sobama...).

Članak 12.

Pravila sigurnog ponašanja:

- Osobne informacije na internetu se nikad 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 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 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, niti je dozvoljeno primati tuđe radove s interneta.

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

Računalni programi su također zaštićeni zakonom kao i jezična djela. Najčešće su zaštićeni samo izvorni programi, no ne i ideje na kojima se oni zasnivaju. U to su uključeni 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

pojedince, 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 videosadržaja. Mnogi online servisi danas omogućuju preuzimanje glazbenih albuma, pjesama, videosadržaja ili pak e-knjiga na nelegalan način. Primjer su klijenti (npr. Torrent) koji omogućuju dijeljenje sadržaja između računala pa se tako dijele najčešće nelegalno nabavljeni videosadržaji te glazbeni sadržaji, ključevi za korištenje različitih aplikacija i drugi digitalni sadržaji koji su zaštićeni autorskim pravima, gdje je izričito zabranjeno daljnje distribuiranje i umnožavanje bez dozvole autora ili bez plaćanja naknade. Postoje i različiti oblici mrežnog servisa koji omogućuju registraciju korisnika za vrlo nisku mjesečnu pretplatu te nude preuzimanje gotovo neograničene količine digitalnog sadržaja koji je zaštićen autorskim pravom, no to je također nelegalno.

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

Članak 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 i intelektualnog vlasništva. Mogu se koristiti materijali s <https://creativecommons.org/licenses/?lang=hr>
3. Učenike i učitelje poučiti 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 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 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.

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, internetsko nasilje 'cyberbullying' je postalo velik problem.

Iako se velika većina incidenata može riješiti neformalnim putem (zvanjem roditelja, slanja djece savjetniku 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.

Edukacija o neprihvatljivom ponašanju provodi 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 prolaze ili uzrokuju male oblike uznemiravanja, a kroz strategiju će se provesti i preventivne mjere suzbijanja nasilja.

Škola se obvezuje da će:

1. Poučiti učenike i učitelje o mogućim oblicima internetskog nasilja.
2. Učenike i učitelje poučiti o tome kako prepoznati internetsko nasilje.
3. Jasno istaknuti prihvatljiva pravila ponašanja te učenike i učitelje poučiti kroz predmet koji koristi tehnologiju
4. Izraditi strategiju odgovora na internetsko nasilje, i to na blaži i teži oblik.

5. Razviti nultu stopu tolerancije na internetsko nasilje.
6. Obilježavati Dane sigurnog korištenja interneta i suzbijanja nasilja kroz kreativne radove.

Korištenje mobilnih telefona – određeno čl. 25 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.

Učenik smije koristiti mobitel tijekom velikog odmora samo ako se radi o hitnom slučaju.

Roditelj ili skrbnik smije komunicirati s učenikom koji je na nastavi samo preko službenog telefona škole.

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.

KLASA: 011-03/23-01/03

URBROJ: 2121-20-23-01

Predsjednica školskog odbora:



Ivana Vladić

Ivana Vladić, prof.