



e-Škole
USPOSTAVA SUSTAVA RAZVOJA
DIGITALNO ZRELIH ŠKOLA
(PILOT PROJEKT)



CARNet

HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

PRAVILNIK O SIGURNOJ I ODGOVORNOJ UPOTREBI
INFORMACIJSKO – KOMUNIKACIJSKE TEHNOLOGIJE
OSNOVNE ŠKOLE VIKTORA KOVAČIĆA
HUM NA SUTLI

**OSNOVNA ŠKOLA VIKTORA KOVAČIĆA
HUM NA SUTLI**

Hum na Sutli 152/1
49231 Hum na Sutli
Tel.: 049/341162
Fax.: 049/341071
e-mail: ured@os-vkovacica-humnasutli.skole.hr

KLASA: 003-05/18-01/1
URBROJ: 2214/02-380-9-18
U Humu na Sutli, 16.02.2018.

Na temelju članka 24. Statuta OŠ Viktora Kovačića Hum na Sutli, Školski odbor na sjednici održanoj 16.02.2018. godine donosi

**PRAVILNIK O SIGURNOJ I ODGOVORNOJ UPOTREBI
INFORMACIJSKO-KOMUNIKACIJSKE TEHNOLOGIJE
U OSNOVNOJ ŠKOLI VIKTORA KOVAČIĆA
HUM NA SUTLI**

Predsjednica Školskog odbora:
Vesna Kunštek, prof.

Vesna Kunštek

**OSNOVNA ŠKOLA
VIKTORA KOVAČIĆA
HUM NA SUTLI**

I. OPĆE ODREDBE

Članak 1.

Ovaj Pravilnik jasno i nedvosmisleno određuje načine prihvatljivog i dopuštenog korištenja IKT resursa Osnovne škole Viktora Kovačića Hum na Sutli (u daljnjem tekstu: Škole).

Članak 2.

Pravilnik vrijedi za sve korisnike IKT infrastrukture Škole i CARNetove mreže.

Članak 3.

Svrha ovog Pravilnika je:

- Utvrditi načine sigurnog i odgovornog korištenja IKT definiranjem sigurnosne politike Škole
- Zaštititi informacijski sadržaj i opremu
- Zaštititi korisnike od različitih vrsta internetskog nasilja
- Definirati sustave i usluge koji su najprikladniji za djecu
- Poticati aktivno sudjelovanje djece u radu s IKT promovirajući sigurno, odgovorno i učinkovito korištenje digitalnih tehnologija u mrežnoj zajednici

Članak 4.

Učenici i svi školski zaposlenici moraju se pridržavati uputa koje im daje školski administrator sustava ili neka druga ovlaštena osoba radi unapređenja sigurnosti školske informatičke opreme i mreže.

II. OSNOVNE SIGURNOSNE ODREDBE

Članak 5.

Sigurnost informacija, infrastrukture te utjecaj ljudskih i drugih resursa na funkcionalnost pojedinih dijelova IKT infrastrukture izuzetno je važna te su svi korisnici dužni poštivati osnovne sigurnosne odredbe.

Članak 6.

Materijalne i nematerijalne resurse izravno povezane s IKT infrastrukturom čine korisnici, oprema, različite vrste informacija, aplikacije koje se koriste u školi.

- Korisnici IKT infrastrukture u školi su učenici, učitelji, ostali djelatnici i povremeni korisnici (gosti) škole.
- IKT infrastrukturom smatra se računalna oprema dobivena u sklopu pilot projekta e-Škole, stara računalna mreža i računalna oprema.
- U školi postoje interne, javne i povjerljive informacije.
- Aplikacije koje Škola koristi su: e-Dnevnik, e-Matica, HUSO admin, Meraki (središnji sustav za upravljanje računalnom mrežom), skup programa Office 2016 i Office 2010.

Članak 7.

Školska oprema se treba čuvati i pažljivo koristiti.

Članak 8.

Tuđi osobni podaci mogu se koristiti isključivo uz prethodno odobrenje.

Članak 9.

(1) U Školi je implementirana integrirani sigurnosni sustav, a mrežnom opremom u školi upravlja se putem središnjeg sustava za upravljanje i nadzor mreže, smještenog u oblaku. Koriste se antivirusni programi, vatrozid te sigurnosna kopija podataka osobno kod učitelja i ostalih zaposlenika u svrhu sigurnosnih mjera zaštite podataka.

(2) Računala koja su na Windows operativnim sustavima posjeduju vatrozid i antivirusni program Microsoft security essentials. Noviji operativni sustavi, poput Windows 10, posjeduju Windows Defender Security Center. Većina mjera zaštite su implementirana kod davatelja internetski usluga (ISP-a - CARNet).

Članak 10.

Zaposlenici su dužni koristiti službenu e-mail adresu (ime.prezime@skole.hr), a posebice u službenoj komunikaciji s nadležnim tijelima i drugim institucijama iz sustava znanosti i obrazovanja.

Članak 11.

Učiteljima i drugim zaposlenicima škole strogo zabranjeno davati učenicima i drugim korisnicima vlastite zaporke i digitalne identitete. To se odnosi na pristup školskim računalima, e-Matici, e-Dnevniku, računovodstvenim programima, knjižničarskim programima i ostalim informacijskim sustavima ili mrežnim aplikacijama koje sadrže osobne podatke djelatnika i/ili učenika.

Članak 12.

Svi zaposlenici škole moraju potpisati izjavu o tajnosti podataka te se moraju pridržavati etičkih načela pri korištenju IKT-a.

Članak 13.

(1) U slučaju nepridržavanja pravila, Škola sankcionira kršenje / nepridržavanje pravila u skladu sa službenim aktima Škole.

(2) Svako ponašanje koje nije u skladu s Pravilnikom prijavljuje se administratoru e-Dnevnika, e-Škole tehničaru ili ravnatelju Škole.

(3) Ozbiljniji incidenti prijavljuju se CARNet-ovom CERT-u, preko obrasca na mrežnoj stranici www.cert.hr

Članak 14.

Školsku IKT infrastrukturu/opremu čine: računala, projektori, pametne ploče, računalna mreža, sustavski i aplikativni softveri i računalni programi te alati za zaštitu infrastrukture/opreme.

Članak 15.

U školi se koriste stolna računala, prijenosna računala, hibridna računala i tableti.

- Stolna računala koriste se u tajništvu, računovodstvu, knjižnici, uredu psihologa te zbornicama i učionicama matične i područnih škola.

- Prijenosna računala koriste ravnateljica, stručne suradnice i učitelji. Hibridna računala koriste učitelji STEM predmeta.

- Tablete, koje je škola dobila u sklopu projekta e-Škole, koriste učitelji te učenici. Tableti za učenike smješteni su u kolicima za punjenje tableta u informatičkoj učionici i mogu se prenositi u druge učionice.

- Dvije učionice u kojima se održava nastava iz STEM predmeta opremljene su pametnim pločama, dok su ostale učionice za potrebe projekcije opremljene LCD projektorima i televizorima.

Članak 16.

Sva računala i ostala IKT oprema moraju biti zavedena na inventurnim listama CARNeta i Škole. Popis računala i ostale IKT opreme ažurira se jednom godišnje, nakon provedenih inventura.

Članak 17.

Računalna mreža se sastoji od novog dijela koji je izgrađen u sklopu projekta e-Škole te starog dijela mreže. Računala u školi su povezana bežično i žičano.

Članak 18.

(1) Računala se bežično spajaju na 19 bežičnih pristupnih točaka. Pristupne točke su smještene u svakoj učionici te u najvažnijim prostorima škole (zbornica, hol).

(2) U bežičnim pristupnim točkama su postavljene tri naziva za pristup bežičnoj mreži (SSID): eduroam, e-Škole i guest.

a) Na *eduroam mrežu* se spajaju učitelji sa svojim školskim ili privatnim uređajima gdje se autentificiraju svojim korisničkim podacima iz AAI@EduHr sustava.

b) *e-Škole bežična 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.

c) *Guest mreža* se koristi za spajanje vanjskih partnera i posjetitelja. Bežična mreža guest je otvorenog tipa, a za autentifikaciju se koristi Captive portal. Partnerima i posjetiteljima koji imaju AAI@edu račun omogućen je pristup na eduroam mrežu uz ograničenje brzine pristupa.

Članak 19.

(1) Određena računala u školi su spojena žičanim načinom spajanja na mrežu. Računala koja su spojena na taj način spojena su na staru mrežnu infrastrukturu.

(2) Računala koja su spojena žičano su sva računala u informatičkoj učionici, računala u uredima (tajništvo, računovodstvo, zbornica, knjižnica, ured psihologa).

Članak 20.

(1) Dio računalne mrežne infrastrukture škola održava sama i/ili uz pomoć vanjskih održavatelja opreme, dok je održavanje mreže instalirane u sklopu projekta e-Škole u nadležnosti CARNeta.

(2) U sklopu projekta e-Škole od osnivača škole (Krapinsko-zagorska županija) imenovan je e-tehničar, koji je zadužen (najviše osam sati mjesečno) za održavanje navedene mrežne infrastrukture.

Članak 21.

(1) Većina računala u školi posjeduje operativni sustav Windows 10 s instaliranim Office 2010 i Office 2016 aktima. Neka prijenosna računala i sva računala u informatičkoj učionici posjeduju Windows 7 operativni sustav s instaliranim Office 2010 i Office 2016 alatima.

(2) Instalirani sustavski programi na školskim računalima preuzeti su isključivo s Microsoft Download Centra (MSDC) kao središnjeg centra za preuzimanje sustavskih i aplikativnih programa u RH za potrebe osnovnih i srednjih škola.

(3) U sustav se prijavljuje AAI@edu korisničkim računom, a na istom mjestu se mogu preuzeti svi navedeni operativni sustavi i office alati s pripadajućim ključevima za aktivaciju.

Članak 22.

Nadzor licenciranja sustavskih i aplikativnih programa koji se koriste u školi vrši se isključivo preko MSDC sustava.

Članak 23.

(1) Instalaciju i održavanje računalnih programa provodi učitelj informatike, e-tehničar i školski administrator.

(2) Kod svih računala je podešeno ažuriranje operativnog sustava i popratnih office alata na automatski.

Članak 24.

(1) Učenici ne smiju sami instalirati programe na računala. Ako se pojavi potreba za instaliranje dodatnog programa, učenik se mora obavezno javiti učitelju informatike / e-Škole administratoru.

(2) Učitelji smiju instalirati isključivo programe koji su vezani za realizaciju sadržaja nastavnog plana i programa.

Članak 25.

Nepridržavanje pravila instaliranja programa može rezultirati disciplinskim mjerama prema zaposlenici Škole ili pedagoškim mjerama prema učenicima sukladno Pravilniku o kriterijima za izricanje pedagoških mjera.

Članak 26.

Zbrinjavanje računalnog otpada vrši se jednom godišnje, preko ovlaštene tvrtke Audio i video servis „Jurinjak“ iz Krapine.

IV. REGULIRANJE PRISTUPA IKT OPREMI

Članak 27.

Kako bi se zaštitila materijalna (IKT oprema) i nematerijalna imovina (informacije i podaci), reguliran je pristup svim IKT resursima.

Članak 28.

(1) Računalnoj mreži u školi mogu pristupiti zaposlenici i učenici škole te svi ostali koji imaju za to dopuštenje.

(2) Bežičnoj mreži se pristupa isključivo preko AAI@EduHr, tj. preko elektroničkog identiteta. Elektronički identitet u sustavu AAI@EduHr je virtualni identitet na CARNet mreži koji dobivaju pojedinačni korisnici iz ustanova članica CARNeta (učenici, učitelji, studenti, profesori i zaposlenici ustanova članica), a koji im omogućuje korištenje CARNetovih usluga.

Članak 29.

(1) U školi je instaliran Meraki MX vatrozid koji sadrži velik broj sigurnosnih mogućnosti od klasičnih funkcionalnosti L3/L4 vatrozida, naprednih (next-gen) funkcionalnosti vatrozida, IPS-a, do mrežnog antivirusa. Osim toga sadrži i mogućnosti klasičnog, tzv. border gateway uređaja namijenjenog za pozicioniranje na perimetru lokalne mreže prema internetu.

(2) Na Meraki MX UTM-u je uključen i IPS (Intrusion Prevention System) modul koji štiti mrežu od različitih napada s Interneta kao i sustav za otkrivanje i blokiranje nepoželjnog Malware-a. U sklopu Meraki mrežnog rješenja integrirano je i MDM rješenje, odnosno sustav za upravljanje klijentskim uređajima kroz Meraki centralizirano web sučelje. Navedeno rješenje omogućuje upravljanje, dijagnostiku i nadzor nad sigurnosnim postavkama klijentske opreme s IOS, android, Windows phone, Windows, Windows Server i MacOS operativnim sustavima.

(3) Osim filtriranja sadržaja, moguće je blokirati pristup pojedinim mrežama korištenjem klasičnih Layer 3 i Layer 7 pristupnih listi (ACL – Access Control List).

(4) Za svaki VLAN konfiguriran na mreži podignut je DHCP server na Meraki MX UTM uređaju. Vrijeme čuvanja IP adrese pojedinom klijentu (Lease time) je 4 sata za VLAN-ove koji se koriste i za bežične klijente te 24 sata za VLAN-ove koji se koriste samo za spajanje žičnih klijenata.

Članak 30.

(1) Za pristup mreži *eSkole* koriste se sljedeći parametri:

- PSK (pre-shared key) za autentikaciju korisnika i pristup na bežičnu mrežu
- WPA2 enkripcija podataka na pristupnom sloju bežične mreže
- Captive portal za autentikaciju korisnika prilikom pristupa internetu
- korisnici nakon pristupa u mrežu *eSkole* pripadaju u VLAN 10 i imaju IP adresu iz mreže

192.168.30.0/23.

(2) Za pristup mreži *eduroam* koriste se sljedeći parametri:

- 802.1X enterprise RADIUS autentikacija, uz WPA2 enkripciju podataka
- za pristup mreži *eduroam* koriste se postavke TTLS-PAP
- korisnici nakon pristupa u mrežu *eduroam* pripadaju u VLAN 14 i imaju IP adresu iz mreže 192.168.38.0/23, osim ako se radi o nastavnicima koji tada pripadaju u VLAN 10 i imaju IP adresu iz mreže 192.168.30.0/23
- za navedenu mrežu se limitira ukupna propusnost na 10% ukupne propusnosti internetske veze, ako se ne radi o nastavnicima, odnosno ako se klijenti pozicioniraju u VLAN 14.

(3) Za pristup *guest* mreži koriste se sljedeći parametri:

- otvoren pristup mreži, uz mogućnost Captive portal autentikacije pristupa na internet
- za autentikaciju se koristi baza korisnika iz Meraki dashboarda
- korisnici nakon pristupa u mrežu *eduroam* pripadaju u VLAN 13 i imaju IP adresu iz mreže 192.168.36.0/23
- za navedenu mrežu se limitira ukupna propusnost na 10% ukupne propusnosti veze prema internetu.

Članak 31.

Preko besplatne Office365 usluge i alata koji omogućuju suradnju i komunikaciju između svih sudionika u obrazovnom sustavu, moguće je koristiti i OneDrive kao način za pohranjivanje sadržaja na oblak. Pristup OneDrive-u za škole moguć je preko AAI@EduHr elektroničkog identiteta.

Članak 32.

(1) Računala u informatičkoj učionici se koriste za vrijeme trajanja nastave informatike i predmeta iz STEM područja. Korištenje opreme u informatičkoj učionici propisano je posebnim pravilima kojih se učenici moraju pridržavati.

(2) Za održavanje i ispravnost opreme u informatičkoj učionici odgovoran je učitelj informatike.

(3) Ostala računala u školi (stolna računala, prijenosna računala i tablete) učenici smiju koristiti za vrijeme nastave ostalih predmeta samo uz odobrenje učitelja.

(4) Učenici smiju pristupiti internetskim sadržajima, npr. pretraživanju interneta, društvenim mrežama i sl. i za vrijeme odmora u školskoj knjižnici, uz prethodno dopuštenje i nadzor knjižničara.

Članak 33.

Učenici uz odobrenje učitelja smiju koristiti svoje privatne uređaje za pristup aplikacijama i internetskim sadržajima koji su u funkciji ostvarenja nastavnih sadržaja.

Članak 34.

Zaporke koje koriste učenici i ostali djelatnici Škole moraju sadržavati brojke i slova te minimalno osam (8) znamenki.

Članak 35.

(1) U Školi se provodi filtriranje nepoćudnih sadržaja. Odlukom Ministarstva znanosti i obrazovanja sve osnovne i srednje škole spojene na CARNet mrežu automatski su uključene i u sustav filtriranja nepoćudnih sadržaja. Odlukom MZO-a onemogućava se prikazivanje 14 kategorija stranica na računalima u osnovnim i srednjim školama (http://www.carnet.hr/filtriranje_sadržaja).

(2) Učenici su obvezni prihvatiti filtriranje određenih sadržaja kao sigurnosnu mjeru te ga ne smiju pokušati zaobići jer je ono postavljeno radi njihove osobne sigurnosti, ali i sigurnosti svih drugih učenika. Zabranjeno je zaobilaženje bilo kojih sigurnosnih postavki računalne opreme.

Članak 36.

Da bi se održao korak s trendovima u korištenju IKT-a, kao i s nadolazećim prijetnjama računalnoj sigurnosti, obavezna je stalna edukacija učenika i cijelog školskog kolektiva vezano uz korištenje IKT.

Članak 37.

(1) Učenici se prijavljuju na računala kao standardni korisnici, a učitelji, stručni suradnici i ravnatelj kao administratori.

(2) Svi korisnici računala moraju se nakon korištenja odjaviti iz svih sustava u koje su se prijavili.

Članak 38.

(1) Zabranjuje se ophođenje s privatnim (i tajnim) podacima koje su korisnici dobili od Škole (poput elektroničkog identiteta u sustavu [AAI@Edu.hri sl.](mailto:AAI@Edu.hri.sl)).

(2) Pokretanje izvšnih datoteka se zabranjuje, osim ako se iznimno pojavi potreba, to mora biti uz dopuštenje e-Škole administratora.

Članak 39.

(1) Elektronički identitet u sustavu AAI@Edu.hr ima oblik ID_korisnika@oznaka_ustanove.hr

(2) Elektronički identitet u sustavu AAI@Edu.hr dodjeljuje administrator elektroničkog (LDAP) imenika škole.

(3) Svi učenici i učitelji dobivaju elektronički identitet koji im se daje na korištenje i čuvanje.

(4) Ukoliko korisnici izgube svoj korisnički račun, javljaju se administratoru koji ispisuje korisnički račun s novom ili starom lozinkom.

(5) U slučaju promjene škole, elektronički identitet učenika se prenosi. Isto vrijedi i za učitelje i ostale zaposlenike škole.

Članak 40.

Učeniku prestaju prava za korištenje AAI@Edu.hr identiteta završetkom školovanja, a zaposlenicima prestankom rada u ustanovi.

1. Ponašanje na internetu

Članak 41.

Svaki pojedinac je odgovoran za svoje ponašanje u virtualnom svijetu, a prema ostalim korisnicima mora ponašati na primjeren način. Zabranjeno je na bilo koji način vrijeđati i zastrašivati korisnike na internetu te objavljivati neprimjerene sadržaje.

Članak 42.

Svaki korisnik interneta dužan je upoznati se s osnovnim pravilima ponašanja u takvom okruženju. Škola je dužna upoznati učenike s pravilima ponašanja na internetu.

Članak 43.

(1) Komunikacija putem interneta opisana je pravilima primjerenog ponašanja u internetskoj komunikaciji pod nazivom 'internetski bonton', ili 'Netiquette'. 'Netiquette' na hrvatskom jeziku dostupan je na <http://hr-netiquette.org> te propisuje smjernice i pravila ponašanja u tri (3) kategorije: elektronička pošta, popis e-adresa i forumi.

(2) Škola je ovaj skup pravila lijepog ponašanja na internetu učinila dostupnim svojim učenicima, o tome ih podučava, te primjenjuje vlastitu politiku u skladu s tim pravilima.

(3) Ovaj skup pravila je sastavni dio Pravilnika te se nalazi u prilogu. Izvješten je u informatičkoj učionici te je objavljen na mrežnoj stranici škole.

Članak 44.

(1) U sklopu redovne nastave te kroz aktivnosti propisane Školskim kurikulumom, učenike se poučava o važnosti čuvanja vlastitih i tuđih osobnih podataka na servisima koji omogućuju komunikaciju između korisnika na internetu.

(2) Osobni podaci su sve informacije putem kojih se osoba može identificirati izravno ili neizravno na način da se njezin identitet može utvrditi na osnovi jednog ili više specifičnih obilježja.

Članak 45.

Osim Pravila lijepog ponašanja na internetu, učenici se moraju pridržavati i *Pravila sigurnog ponašanja na internetu*:

- Osobne informacije na internetu se nikad ne smiju odavati.
- Tvoja zaporka je tvoja tajna. Ne dijeli je sa svojim prijateljima i poznanicima.
- Ne odgovarajte na zlonamjerne ili prijeteće poruke.
- Dokaze neprimjerenog sadržaja spremite (print screen) i pokažite odraslim osobama.
- Zlostavljanje preko interneta se ne smije prikrivati. Zlostavljanje treba prijaviti odraslim osobama u okolini i platformi na kojoj se zlostavljanje odvija.
- Provjerite je li profil na društvenim mrežama zatvoren 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 društvenim mrežama. Nikad ne objavljuj fotografije drugih osoba bez njihovog pristanka.
- Redovito provjeravaj postoji li neka mrežna stranica o tebi te koje informacije sadrži (treba upisati svoje ime i prezime u Google).
- Ne prihvaćaj poklone od nepoznatih osoba na internetu (npr. bon). Ta osoba zasigurno želi nešto zauzvrat.
- Nikad nemoj ići sam na sastanak s osobom koju si upoznao putem interneta. Ako ta osoba inzistira da dođeš bez pratnje, nemoj ići na takav sastanak te obavezno obavijesti roditelja.

2. Poštivanje autorskih prava

Članak 46.

- (1) 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 su skup autorsko-pravnih licenci pravovaljanih u čitavom svijetu. Pomažu autorima da zadrže svoja autorska prava te reguliraju legalne načine korištenja njihova djela.
- (2) Učitelji, učenici i ostali djelatnici se potiču da potpisuju vlastite materijale koji su sami izradili koristeći CC licencu.
- (3) Zaposlenici i učenici Škole obavezuju se na poštivanje CC licenca.

Članak 47.

- (1) Zabranjuje se predstavljanje tuđih radova kao svojih, preuzimanje zasluga za tuđe radove i nedopušteno preuzimanje tuđih radova s interneta.
- (2) Korištenje tuđih materijala s interneta mora biti citirano, obavezno navodeći autora korištenih materijala te izvor informacije (poveznica i datum preuzimanja).

Članak 48.

- (1) Računalni programi su zaštićeni zakonom kao jezična djela. Najčešće su zaštićeni samo izvorni programi, no ne i ideje na kojima se oni zasnivaju. U to su uključeni i mrežni programi, odnosno aplikacije.
- (2) Kod mrežnog mjesta je moguće 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.

3. Dijeljenje datoteka

Članak 49.

- (1) Prilikom dijeljenja tuđeg digitalnog sadržaja potrebno je poštivati autorska prava osobe te sadržaj dijeliti u skladu s dodijeljenom licencom (Creative Commons).
- (2) Vlastitim sadržajima potrebno je dodijeliti prikladnu licencu prije dijeljenja te zaštititi autorska prava.

Članak 50.

U školi se zabranjuje nelegalno kopiranje ili preuzimanje autorski zaštićenog materijala. Kako bi se spriječilo nelegalno preuzimanje sadržaja računalna mreža je postavljena tako da u potpunosti onemogućava P2P (peer to peer) protokole i filtrira mrežne stranice koje sadrže P2P datoteke (tzv. Torrenti).

Članak 51.

Obaveze Škole su:

1. Učenike i učitelje podučiti o autorskom pravu i intelektualnom vlasništvu.
2. Učenike i učitelje podučiti i usmjeriti na korištenje licenci za zaštitu autorskog prava i intelektualnog vlasništva.
3. Učenike i učitelje podučiti o načinima nelegalnog dijeljenja datoteka i servisima koji to omogućuju poput Torrent servisa, mrežnog mjesta koja zahtijevaju registraciju i plaćanje vrlo niske članarine za neograničeno preuzimanje digitalnog sadržaja i sl.
4. Učenike i učitelje informirati o mogućim posljedicama nelegalnog korištenja, dijeljenja i umnažanja autorski zaštićenih materijala.

4. Internetsko nasilje

Članak 52.

(1) Internetsko nasilje može se 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 informacijsko komunikacijskom tehnologijom koja se može smatrati štetnom kako za pojedinca, tako i za opće dobro.

(2) Internetskim nasiljem smatra se:

- nastavljanje slanja e-pošte usprkos tome što netko više ne želi komunicirati s pošiljateljem
- slanje poruka prijetećeg ili uvredljivog sadržaja
- omalovažavanje ili ismijavanje uz pomoć različitih servisa koji omogućuju komunikaciju (društvene mreže, forumi, video poziv, chat...)
- dijeljenje tuđih osobnih podataka i drugih informacija o drugoj osobi
- objavljivanje fotografija i video sadržaja koji mogu nanijeti štetu osobi
- objavljivanje slika i videa nasilnog sadržaja
- lažno predstavljanje i krađa identiteta
- otvaranje grupa s ciljem vrijeđanja i omalovažavanja
- postavljanje internetske ankete o žrtvi
- slanje virusa
- svi ostali oblici nasilja posredovani IKT-om

Članak 53.

- (1) Ukoliko se utvrdi postojanje internetskog nasilja, osoblje škole mora djelovati s ciljem prekidanja nasilne situacije.
- (2) Potrebno je u najkraćem mogućem roku maknuti neprihvatljiv sadržaj s interneta. Osoblje škole obavlja razgovor sa učenicima uključenima u nasilje putem interneta te obavještava roditelje.
- (3) Učenici će biti sankcionirani sukladno Pravilniku o pedagoškim mjerama.

Članak 54.

Škola je dužna:

1. Podučiti učenike i nastavnike o načinima prepoznavanja i mogućim oblicima internetskog nasilja.
2. Upoznati učenike i jasno istaknuti prihvatljiva pravila ponašanja u školskom prostoru te na web stranici škole.
3. Kontinuirano educirati učenike i roditelje o sigurnom korištenju interneta i suzbijanja nasilja

5. Korištenje mobilnih telefona

Članak 55.

- (1) Kućnim redom škole zabranjeno je korištenje mobitela za vrijeme trajanja nastave i organiziranih aktivnosti.
- (2) Korištenje mobitela za potrebe nastavnog procesa moguće je uz prethodno dopuštenje učitelja.
- (3) U slučaju nedopuštenog korištenja mobitela i druge tehnologije učitelj učeniku oduzima mobitel do kraja trajanja nastave. Obavještava se roditelja o nedopuštenom korištenju mobitela.
- (4) Ako učenik ponovno koristi mobitel ili drugu tehnologiju na nastavi, isti se oduzima i obavještava roditelj koji je dužan doći po uređaj.

Članak 56.

Mobilni telefoni imaju pristup internetu te su sigurnosne mjere za korištenje interneta navedene u člancima 41. -45. obvezujuće i za korištenje mobilnih telefona.

Članak 57.

- (1) Škola je dužna upoznati učenika s posljedicama zloupotrebe mobitela.
- (2) Roditelji se informiraju o sigurnim načinima korištenja mobitela na roditeljskim sastancima ili kroz edukativne publikacije koje pripremi Škola ili druga ovlaštena institucija.

VII. PRIJELAZNE I ZAVRŠNE ODREDBE

Članak 58.

Izrazi koji se rabe u Pravilniku, a imaju rodno značenje, rabe se neutralno i odnose se na muški i ženski spol.

Članak 59.

Ovaj Pravilnik stupa na snagu danom donošenja, te se objavljuje na web stranici Škole.