

Republika Hrvatska
Zadarska županija
OŠ Jurja Dalmatinca Pag
Ante Starčevića 12
23 250 PAG

**PRAVILNIK O SIGURNOJ I ODGOVORNOJ UPOTREBI
INFORMACIJSKO-KOMUNIKACIJSKE TEHNOLOGIJE OSNOVNE
ŠKOLE JURJA DALMATINCA PAG**

Sadržaj

1. Uvod	3
2. Osnovne sigurnosne odredbe	5
3. Školska IKT oprema i održavanje.....	7
4. Reguliranje pristupa IKT opremi.....	9
5. Sigurnost korisnika	12
6. Prihvatljivo i odgovorno korištenje informacijsko-komunikacijske tehnologije ...	13
6.1. Ponašanje na internetu	13
6.2. Autorsko pravo	14
6.3. Dijeljenje datoteka	15
6.4. Internetsko nasilje	15
6.5. Korištenje mobilnih telefona.....	16

1. Uvod

Na temelju odredbe članka 58. Statuta Osnovne škole Jurja Dalmatinca Pag, (KLASA: 012-03/18-01/01, URBROJ: 2198-1-27-01-18-02) od 21. veljače 2018. godine, te odredbe članka 118. stavka 2. Zakona o odgoju i obrazovanju u osnovnoj i srednjoj školi (NN 87/08, 86/09, 92/10, 105/10, 90/11, 5/12, 16/12, 86/12, 126/12, 94/13, 152/14 i 07/17) Školski odbor Osnovne škole Jurja Dalmatinca Pag, a na prijedlog ravnateljice Željke Zubović na elektronskoj sjednici održanoj 19. ožujka 2018. godine, donosi

PRAVILNIK O SIGURNOJ I ODGOVORNOJ UPOTREBI INFORMACIJSKO-KOMUNIKACIJSKE TEHNOLOGIJE OSNOVNE ŠKOLE JURJA DALMATINCA PAG

Članak 1.

S obzirom na sve veću sustavnu uporabu IKT-a 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.). Potrebno je veliku pozornost 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 je dio sigurnosne politike škole. Oblikovan je uzimajući u obzir preporuke EACEA7Eurydice mreže(<http://eurydice.hr>) koja analizira i pruža informacije o europskim obrazovnim sustavima, a usmjerena je na strukturu i organizaciju obrazovanja u Europi na svim razinama.

Članak 2.

Pravilnik je donesen sa svrhom:

- unaprjeđenja sigurnosti školske informatičke opreme i mreže,

- jasnog i nedvosmislenog o određivanja načina prihvatljivog i dopuštenog korištenja IKT resursa škole
- zaštite informacijskog sadržaja i opreme,
- zaštite korisnika od različitih vrsta internetskog zlostavljanja,
- promoviranja sustava i usluga koji su najprikladniji za djecu,
- poticanja aktivnog sudjelovanja djece u radu s IKT-om promovirajući sigurno, odgovorno i učinkovito korištenje digitalnih tehnologija u mrežnoj zajednici pravilne raspodjele zadataka i odgovornosti nadležnih osoba,
- propisivanja sankcija u slučaju kršenja odredbi Pravilnika

U školi je u kolovozu 2017. godine postavljena infrastruktura CARNetove mreže.

Pravilnik vrijedi za sve korisnike IKT infrastrukture škole.

Članak 3.

U Osnovnoj školi Jurja Dalmatinca e-škole tehničarem imenovan je Joško Žepina, Adriatic info, Zadar.

Administrator resursa je učitelj informatike Šime Gligora. Administrator imenika je tajnik Mladen Stupičić.

Školski djelatnici moraju pridržavati uputa koje im može dati školski administrator radi unapređenja i održavanja sigurnosti školske informatičke opreme i mreže.

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

2. Osnovne sigurnosne odredbe

Članak 4.

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

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

Materijalni resursi su:

- Kompletna računalna mreža izgrađena u sklopu projekta e-Škole i računalna oprema,
- Stara računalna mreža i računalna oprema

Nematerijalni resursi su:

- Aplikacije koje škola koristi: e-dnevnik, e-matica, Obračun plaća s evidencijom kadrova,
- Meraki (središnji sustav za upravljanje računalnom mrežom)
- Web stranica škole <http://www.os-jdalmatinca-pag.skole.hr/>

Školska oprema se mora čuvati i pažljivo koristiti.

Članak 5.

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

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

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

Članak 6.

Sva računala koja su na Windows operativnim sustavima(Windows 7 i noviji) i posjeduju ugrađeni antivirusni program (Windows Defender Security) i ugrađeni vatrozid.

Školski davatelj internetski usluga (ISP-a) je CARNet. Preko njega su implementirane mjere zaštite pristupa i korištenja internetskih servisa.

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

Sigurnosne kopije se izrađuju samo na računalima u knjižnici, tajništvu i računovodstvu i izrađuju ih djelatnici.

Učiteljima i drugim djelatnicima je strogo zabranjeno davati učenicima i drugim korisnicima vlastite zaporke i druge digitalne identitete.

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.

3. Školska IKT oprema i održavanje

Članak 7.

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

U sklopu e-Škole projekta od osnivača škole imenovan je e-tehničar koji je zadužen i plaćen za održavanje navedene mrežne infrastrukture.

Računala se bežično spajaju na 15 bežičnih pristupnih točaka. Pristupne točke su smještene u svakoj učionici te u najvažnijim prostorima škole (zbornica, hol, dvorana).

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

- a) Eduroam - mrežu se spajaju učitelji i učenici sa svojim privatnim ili školskim uređajima gdje se autentificiraju svojim korisničkim podacima iz AAI@EduHr sustava. Na taj način se može identificirati i pratiti njihov promet u računalnoj mreži.
- b) eSkole - 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
- a) 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. 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.

Određena računala u školi su spojena žičanim načinom spajanja na mrežu.

Računala koja su spojena žičano su sva računala u informatičkoj učionici, računala u uredima (ured ravnatelja, tajništvo, računovodstvo, zbornica, knjižnica, ured defektologa). Računalna mreža je konfigurirana tako da nema potrebe da se računala/korisnici autentificiraju kada se spajaju u žičanu računalnu mrežu.

Članak 8.

Većina računala u školi posjeduje operativni sustav Windows 10 s instaliranim Office 2010,2013 ili 2016 Office alatima. Sva računala u informatičkoj učionici posjeduju Windows 10 operativni sustav. Kod svih računala je podešeno ažuriranje operativnog sustava i popratni office alata na automatski. Operativni sustavi Windows 10 imaju u sebi sigurnosni sustav (Windows Defender Security Center) te također i vatrozid.

Filtriranje sadržaja je u skladu sa postavkama CARNet-a kao pružatelja usluga Interneta.

Trenutno u školi nema potrebe samostalnog nadziranja licenciranih programa jer svi programi koji se koriste (Windows XP, 7, 8, 8.1, 10, Office 2007, 2010, 2013, 2016) 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 (administrator resursa, e-tehničar). U sustav se prijavljuje AAI@edu korisničkim računom gdje se mogu preuzeti svi navedeni operativni sustavi i office alati s pripadajućim ključevima za aktivaciju.

Članak 9.

Na računala u školi učenici ne smiju ništa instalirati bez odobrenja administratora resursa ili e-tehničara. Ako se pojavi potreba za instaliranje dodatnog programa korisnik se mora obavezno javiti administratoru resursa ili e-tehničaru.

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

4. Reguliranje pristupa IKT opremi

Članak 10.

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 postavljene tri naziva za pristup bežičnoj mreži (SSID):

- a) eduroam - Na eduroam mrežu se spajaju učitelji i učenici sa svojim privatnim ili školskim uređajima gdje se autentificiraju svojim korisničkim podacima iz AAI@EduHrsustava (802.1x with custom RADIUS enkripcija). Na taj način se može identificirati i pratiti njihov promet u računalnoj mreži.
- b) e-Skole 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).
- c) Guest mreža se koristi za spajanje vanjskih partnera i posjetitelja (Open-passwordprotected 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 11.

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

Učitelji 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 računalima u informatičkoj učionici postavljeno je da se kod prijave u operativni sustav koristi zaporku, a učenici nemaju administratorska prava.

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

Članak 12.

Na učiteljevom računalu u učionici informatike nalazi se prostor za zajedničko dijeljenje dokumenata. Učenici svoje dokumente spremaju na prijenosne memorije. Ukoliko učenici spremaju dokumente lokalno na računalo, nitko ne preuzima odgovornost za gubitak podataka. Pristup aplikacijama i internetskim sadržajima/servisima određuje isključivo učitelj.

Vlastita računala i pametne telefone učenici smiju za vrijeme nastave koristiti isključivo u obrazovne svrhe i uz prethodnu dozvolu učitelja, pri čemu moraju paziti da ne ugrožavaju druge korisnike školske mreže širenjem virusa i drugih zlonamjernih programa.

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

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

Svi učitelji koji koriste informatičku učionicu moraju se držati navedenog:

- učionica mora ostati na kraju onako kako je i zatečena
- računala se obavezno moraju ugasiti nakon uporabe
- u slučaju da računalo ne radi ili je prestalo raditi tijekom sata – obavijestiti ravnateljicu kao nadležnu osobu ili administratora
- radna mjesta moraju ostati čista
- radno mjesto mora ostati uredno – namještena tipkovnica, miš, monitor, stolica na svojem mjestu
- prozore obavezno zatvoriti
- učionicu zaključati

Računalima u informatičkoj učionici pristupa se preko dva računa. Jedna račun koristi administrator, a drugi koriste učenici. Račun administratora zaštićen je lozinkom, dok račun za učenike nije zaštićen lozinkom.

Preporučuje se korištenje korisničkih zaporki koje se sastoje od kombinacije malih i velikih slova, brojeva i posebnih znakova te su minimalne duljine 8 znakova.

Članak 13.

Odlukom Ministarstva znanosti i obrazovanja sve osnovne i srednje škole spojene na CARNet mrežu automatski su uključene i u sustav filtriranja nepoćudnih sadržaja. Od učenika se očekuje da prihvate filtriranje određenih sadržaja kao sigurnosnu mjeru te ga ne smiju pokušati zaobići, jer je ono postavljeno radi njihove sigurnosti, ali i sigurnosti svih drugih učenika. Nadalje, zaobilazanje sigurnosnih postavki moglo bi ugroziti održavanje nastave.

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

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

5. Sigurnost korisnika

Članak 14.

U školama je potrebna neprekidna edukacija učenika, učitelja i cijelog školskog kolektiva kako bi se mogao održati korak u korištenju IKT-a, kao i s nadolazećim prijetnjama u računalnoj sigurnosti.

Prilikom korištenja računala i programi koji zahtijevaju prijavu lozinkom, potrebno je voditi računa da se kod prijave ne otkriju podaci o prijavi. Kada učenici odlaze iz učionice, a ostavljaju računalo uključeno, nastavnici su dužni odjaviti ih iz svih sustava u koje su se prijavili.

Članak 15.

Učenici koji koriste računala u STEM učionicama, dužni su se obvezno nakon završetka rada odjaviti iz sustava u koje su se prijavili.

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

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

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

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

Dopušteno je preuzimanje datoteka na lokalna računala te pokretanje izvršnih datoteka. Ako se utvrdi da se na taj način računala inficiraju zlonamjernim programima, e-tehničar će uvesti restrikciju na takvu vrstu interakcije.

Škola ne revidira elektroničke identitete učenika tijekom školovanja. U slučaju gubitka ili potrebe za promjenom podataka učenici se moraju javiti administratoru imenika.

6. Prihvatljivo i odgovorno korištenje informacijsko-komunikacijske tehnologije

6.1. Ponašanje na internetu

Članak 16.

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

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

Pravila poželjnog ponašanja 'Netiquette' dostupna su na <http://hr-netiquette.org>. Osim Pravila poželjnog ponašanja na internetu, uputno je da se učenici pridržavaju i sljedećih naputaka (Pravila sigurnog ponašanja):

- Osobne informacije na internetu se nikad ne smiju odavati.
- Zaporka je tajna i nikad se ne smije nikome reći.
- Ne 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.
- Treba provjeriti je li Facebook profil skriven za osobe koji nam nisu 'prijatelji'.
- Treba biti kritičan prema ljudima koji se primaju za 'prijatelje'.
- Potrebno je biti oprezan s izborom fotografija koje se objavljuju na Facebooku.
- Treba provjeriti postoji li neka mrežna stranica o nama te koje informacije sadrži (treba upisati svoje ime i prezime u Google).

Učenike se poučava kroz nastavu informatike i satova razrednika da ne otkrivaju osobne podatke, svoju adresu, ime škole, telefonske brojeve i slično preko interneta (na servisima poput Facebooka, Twitera, chat sobe...).

6.2. Autorsko pravo

Članak 17.

Učitelji, učenici i ostali djelatnici se potiču da potpisuju materijale koji su sami izradili koristeći neku licencu te da poštuju tuđe radove.

Nipošto ne smiju 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 naravno ion-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.

6.3. Dijeljenje datoteka

Članak 18.

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

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

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

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

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

6.4. Internetsko nasilje

Članak 19.

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

Postoje različiti oblici internetskog zlostavljanja:

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

- otkrivanje osobnih podataka žrtve na mrežnim stranicama ili forumima,
- lažno predstavljanje žrtve na internetu,
- slanje prijetećih poruka žrtvi koristeći različite internetske servise (poput Facebooka, Skypea, e-maila i drugih servisa za komunikaciju),
- postavljanje internetske ankete o žrtvi,
- slanje virusa na e-mail ili mobitel,
- slanje uznemirujućih fotografija putem e-maila, mms-a ili drugih komunikacijskih alata.

Nedopušteni su svi oblici nasilničkog ponašanja te će svi oni za koje se utvrdi da provode takve aktivnosti biti sankcionirani u skladu s Pravilnikom o kriterijima za izricanje pedagoških mjera i Kućnim redom Škole.

6.5. Korištenje mobilnih telefona

Članak 20.

Korištenje mobilnih telefona za vrijeme nastave propisano je Kućnim redom škole.

Učenici mogu koristiti mobitel u slobodno vrijeme (mali odmor, veliki odmor) poštujući odredbe Pravilnika i Kućnog reda. Iznimno, učenici mogu koristiti mobitele (smartphone) za vrijeme nastave kao nastavno pomagalo kada učitelj to zatraži i pravovremeno najavi. Svaka upotreba tehnologije u učionici mora imati unaprijed zadanu 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.

Članak 21.

Ovaj Pravilnik stupa na snagu danom donošenja te se objavljuje na mrežnom mjestu škole.

Na temelju članka 58. Statuta Osnovne škole Jurja Dalmatinca, Školski odbor na sjednici održanoj 19. ožujka 2018. godine donosi Pravilnik o sigurnoj i odgovornoj upotrebi informacijsko-komunikacijske tehnologije

KLASA: 012-03/18-01/01

URBROJ: 2198-1-27-01-18-03

Pag, 19. ožujka 2018. godine

Predsjednik Školskog odbora

Anthony Buljanović
