OŠ VIKTORA CARA EMINA, LOVRAN
ŠKOLSKI ODBOR
KLASA:003-06/18-01/02
URBROJ: 2156-26-01-18-04

PRAVILNIK O SIGURNOJ I ODGOVORNOJ UPOTREBI INFORMACIJSKO-KOMUNIKACIJSKE TEHNOLOGIJE OSNOVNE ŠKOLE VIKTORA CARA EMINA, LOVRAN

Lovran, ožujak 2018. godine

Na temelju članka 60. Statuta škole, na 14. sjednici održanoj dana 15.03.2018. godine, Školski odbor donosi Pravilnik o sigurnoj i odgovornoj upotrebi informacijsko-komunikacijske tehnologije (dalje u tekstu: IKT)

I. UVOD

Članak 1.

Zbog sve veće sustavne uporabe IKT-a u školama, nužno je voditi računa o prijetnjama informacijskom sadržaju i IKT strukturi a što može rezultirati različitim oblima štete informacijskom sustavu škole kao što je gubitak informacija, nemogućnost pristupa resursima i informacijskom sadržaju te uništenju opreme. Iz tog razloga potrebno je pozornost posvetiti sigurnom i odgovornom korištenju IKT-a.

Odredbe ovog Pravilnika primjenjuju se na sve korisnike IKT.

Članak 2.

Tijekom 2017. godine postavljena je infrastruktura CARNet-ove mreže. Učenici, nastavnici i svi djelatnici škole moraju se pridržavati uputa koje im je dao e-Škole tehničar, Dražen Zrinšćak.

Pravilnik o sigurnoj i odgovornoj upotrebi IKT je dio sigurnosne politike škole. Oblikovan je uzimajući u obzir preporuke EACEA7Eurydice mreže (http://aurydice.hr) koja analizira i pruža informacije o europskim obrazovnim sustavima, a usmjerena je na strukturu i organizaciju obrazovanja u Europi na svim razinama.

Svrha donošenja Pravilnika je:

- nedvosmisleno i jasno odrediti načine prihvatljivog i dopuštenog IKT resursa Škole,
- unaprijediti sigurnost školske informatičke opreme i mreže,
- zaštititi informacijski sadržaj i opremu,
- zaštititi korisnike od različitih vrsta internetskog zlostavljanja,
- promovirati sustav i usluge koji su najprikladniji za djecu,
- poticati aktivno sudjelovanje djece u radu s IKT-om promovirajući sigurno, odgovorno i učinkovito korištenje digitalnih tehnologija u mrežnoj zajednici,
- propisivati sankcije u slučaju kršenja odredbi Pravilnika.

II. OSNOVNE SIGURNOSNE ODREDBE

Članak 3.

Materijalni i nematerijalni resursi su:

- Računalna mreža izrađena u sklopu pilot projekta e-Škole te računalna oprema dobivena u sklopu pilot projekta,
- Školska računalna mreža i oprema
- Aplikacije koje škola koristi: e-Dnevnik, e-Matica, HUSO-admin, Meraki (središnji sustav za upravljanje računalnom mrežom), COP-registar zaposlenih i obračun plaća, Riznica PGŽ te Microsoft Office skup programa.
- Korisnici IKT infrastrukture: učenici, nastavnici, ostali zaposleni te povremeni korisnici (gosti).

Članak 4.

Školska oprema s 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 (kontakt podaci osobe, fotografije i sl.) 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 ta to opunomoći.

Članak 6.

Sva računala su opremljena Windows Defender antivirusnim programom koji je ujedno i vatrozid. Program se ažurira redovito i automatske zbog novih definicija virusa. Škola nema sigurnosnu kopiju podatka osim u računovodstvu. Zaštita pružena spajanjem AAI@Edu korisničkim računom na mrežu nije kontrolirana od strane škole.

Svi zaposlenici 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.

Nastavnicima 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 CARNet-ovu CERT-u preko obrasca na mrežnoj stranici www.cert.hr.

III. ŠKOLSKA IKT OPREMA I ODRŽAVANJE

Članak 7.

Računala u školi su povezana bežično i žičano. U školi se računalna mreža sastoji od novog dijela koji je izgrađen u sklopu projekta e-Škole te starog dijela mreže. U sklopu e-Škole od osnivača škole Primorsko-goranske županije imenovan je e-tehničar koji je zadužen za održavanje naveden mrežne infrastrukture.

Računalni otpad odvozi ovlaštena tvrtka „Metis“ iz Rijeke.

Članak 8.

Računala se bežično spajaju putem bežičnih pristupnih točaka. Pristupne točke smještene su u svakoj učionici te u zbornici, knjižnici, sportskoj dvorani i prostoriji za produženi boravak.

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

a) eduroam,
b) eSkole
c) guest

Članak 9.

Određena računala u školi spojena su žičanim načinom spajanja na mrežu i ta računala su spojena na staru mrežnu infrastrukturu. Računala koja su spojena žičano su računala u uredima ravnateljice, tajništva, računovodstva, zbornice, defektologa i psihologa. Računalna mreža je konfigurirana tako da nema potrebe da se računala autentificiraju kada se spajaju u žičanu računalnu mrežu.

Članak 10.

Većina računala u školi posjeduje operativni sustav Windows 10 s instaliranim Office 2016 alatima. Neka računala posjeduju Windows 7 s instaliranim Office 2010 alatima. Postavke na računalima su podešene na općenite te je na svim računalima postavljeno da kod prijave u operativni sustav nema zaporke. Također je uključena opcija da lozinka nikada ne ističe (Password never expires). Kod svih računala je podešeno ažuriranje operativnog sustava i popratnih office alata na automatski. Računalna mreža pokazuje da najveći promet, koji računala ostvaruju preko interneta, odlazi na ažuriranje navedenog. Operatinvi sustavi Windows 10 imaju u sebi obrambeni sustav (Windows Defender Security Center) te također i vatrozid koji posjeduju i stariji operativni sustavi. Antivirusni programi se koriste na starijim operativnim sustavima i to besplatne inačice antivirusnih programa. 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 su licencirani od strane Ministarstva znanosti i obrazovanja i tvrtke Microsoft.

Članak 11.

Učenici ne smiju instalirati nikakve računalne programe u informatičkokj učionici (igrice isl.).

Na ostala računala u školi ne smije se ništa instalirati bez odobrenja administratora. Ako se pojavi potreba za instaliranje dodatnog programa nastavnik/učenik se mora obavezno javiti administratoru.

Članak 12.

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

IV. REGULIRANJE PRISTUPA IKT OPREMI

Članak 13.

Računalnoj mreži mogu pristupiti učenici, nastavnici, ostali djelatnici škole te vanjski 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):

1. eduroam – na tu mrežu spajaju se nastavnici i učenici sa svojim privatnim ili školskim uređajima.
2. 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).

Također 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.

3. 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 autentifikaciju se koristi tzv. Captive portal. Kako bi im se omogućio pristup, e-Škole tehničar u Meraki upravljačkoj ploči mora kreirati korisničko ime za svakog korisnika kojem škola odobri pristup mreži.

U sklopu projekta e-Škole, nastavnici i stručni suradnici zaduženi su opremom (hibridna računala, tableti i prijenosna računala).

U slučaju duže odsutnosti djelatnika, a u svrhu normalnog funkcioniranja nastavnog procesa, djelatnik je dužan vratiti opremu, o čemu odluku donosi ravnatelj.

Članak 14.

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

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. Kojim aplikacijama i internetskim sadržajima učenici mogu pristupiti određuje isključivo učitelj.

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

Članak 15.

Osim računalima koja su dobili u sklopu pilot projekta e-Škole učitelji imaju pristup računalu u zbornici te, prema potrebi računalima u informatičkoj učionici, a administrativno osoblje računalima u uredima Škole.

Članak 16.

Svi nastavnici koji koriste informatičku učionicu moraju se pridržavati sljedećih naputaka:

- Učionica mora ostati na kraju nastave onakva kakva je i zatečena,
- Računala se obavezno moraju ugasiti nakon uporabe,
- U slučaju da neko od računala ne radi ispravno, kontaktirati voditelja informatičke učionice,
- Radna mjesta moraju ostati uredna,
- Prozore obavezno zatvoriti i zaključati učionicu.

Učitelj informatike je odgovora za informatičku učionicu.

Članak 17.

U Školi su sva računala podešena tako da se za ulaz u operativni sustav koristi zaporka. Također je uključena opcija u operativnom sustavu da lozinka nikada ne prestaje (password never expires).

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 18.

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, zaobilaženje sigurnosnih postavki moglo bi ugroziti održavanje nastave.

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

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

V. SIGURNOST KORISNIKA

Članak 19.

U Školi je potrebna neprekidna edukacija učenika, učitelja i ostalih djelatnika kako bi se održao korak u korištenju IKT-a, kao i upozorili o nadolazećim prijetnjama u računalnoj sigurnosti. Prilikom korištenja računala i programa 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, učitelji su dužni odjaviti ih iz svih sustava u koje su se prijavili.

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

Članak 20.

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

Početkom 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, učenika se treba javiti administratoru imenika. Kada učenik prelazi u Školu iz druge Škole, njegov elektronički identitet se prenosi.

Minimalno jednom godišnje potrebno je revidirati elektroničke identitete učenika.

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

Pravila pristupa učenika i djelatnika Škole školskim računalima potrebno je redovito provjeravati i po potrebi mijenjati.

Članak 21.

Datoteke preuzete iz nekog vanjskog izvora (putem elektroničke pošte, vanjskog diska, interneta) mogu ugroziti sigurnost učenika odnosno učitelja. Zato je uputno ne otvarati ili prosljeđivati zaražene datoteke i programe kao niti otvarati datoteke iz sumnjivih ili nepoznatih izvora. Sve takve datoteke potrebno je provjeriti antivirusnim alatom prije korištenja.

VI. PRIHVATLJIVO I ODGOVORNO KORIŠTENJE INFORMACIJSKO-KOMUNIKACIJSKE TEHNOLOGIJE

Članak 22.

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.

Škola će korisnike upoznati s pravilima poželjnog ponašanja na internetu „Netiquette“, objavljivanjem navedenih pravila u informatičkoj učionici.

Članak 23.

Učenici se, osim Pravila poželjnog ponašanja na internetu, trebaju pridržavati i sljedećih naputaka (Pravila sigurnog ponašanja):

- Nikad ne odavati osobne informacije na internetu,
- Zaporka je tajna i ne smije se nikome reći,
- Ne odgovarati na zlonamjerne ili prijeteće poruke,
- Treba pomoći prijateljima koji su zlostavljani preko interneta tako da se to ne prikriva i odmah obavijestiti odrasle,
- Provjeriti je li Facebook profil skriven za osobe koje nam nisu „prijatelji“,
- Biti oprezan s izborom fotografija koje se objavljuju na Facebook-u,
- Provjeriti postoji li neka mrežna stranica o nama te koje informacije sadrži (treba upisati svoje ime i prezime u Google).

Članak 24.

Računalni programi su zaštićeni zakonom kao jezična djela. Najčešće su zaštićeni samo izvorni program ne ne i ideje na kojim se oni zasnivanju a u što su uključeni i on-line programi odnosno web aplikacije.

Korištenje tuđih materijala s interneta mora biti citirano uz obavezno navođenje autora te izvor informacije.

Članak 25.

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 video sadržaja).

Učenike i učitelje treba upozoriti na autorsko pravo i intelektualno vlasništvo te ih usmjeriti na korištenje licenci za zaštitu autorskog prava i intelektualnog vlasništva.

Učenike i učitelje upozoriti na načine nelegalnog dijeljenja datoteka i servisima koji to omogućuju.

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

Članak 26.

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

Neki od najčešćih oblika internetskog zlostavljanja su:

- Nastavljanje slanja e-pošte usprkos tome što netko više dne želi komunicirati s pošiljateljem,
- Otkrivanje osobnih podataka žrtve na mrežnim stranicama ili forumima,
- Lažno predstavljanje žrtve na internetu,
- Slanje prijetećih poruka žrtvi preko Facebooka, Skypea, e-maila i drugih komunikacija),
- Postavljanje internetske ankete o žrtvi,
- Slanje virusa na e-mail ili mobitel,
- Slanje uznemirujućih fotografija putem komunikacijskih alata.

Članak 27.

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 pedagoškim mjerama i Kućnim redom Škole.

Sve učenike i učitelje je potrebno poučiti mogućim oblicima internetskog nasilja te o tome kako prepoznati internetsko nasilje.

U Školi je potrebno razviti nultu stopu tolerancije na internetsko nasilje.

Članak 28.

Kućnim redom Škole zabranjeno je korištenje mobilnih telefona za vrijeme nastave.

Iznimno, učenici mogu koristiti mobilne telefone za vrijeme nastave, kada učitelj to zatraži ili pravovremeno najavi.

Učenici mogu u Školi koristiti mobilne telefone za vrijeme odmora, prije ili poslije nastave, poitujući odredbe Kućnog reda Škole i ovog Pravilnika.

S obzirom na to da mobilni telefoni sve više imaju pristup internetu ste ih djeca koriste za pretraživanje interneta, sigurnosne mjere za korištenje interneta postaju važne i za korištenje mobilnih telefona (zaštita osobnih podataka, izbjegavanje štetnih sadržaja, zaštita potrošača, ovisnost o računalnim igrama i sl.).

Škola će upoznati učenike s posljedicama zlouporabe mobilnih telefona. Nasilje među vršnjacima uključuje bilo kakav oblike poruke zbog koje se osoba osjeća neugodno ili joj se prijeti (tekstualna poruka, videoporuka, fotografija, poziv), odnosno kojoj je cilj uvrijediti, zaprijetiti ili nanijeti bilo kakvu štetu vlasniku mobilnog telefona.

Članak 29.

Ovaj Pravilnik stupa na snagu danom donošenja i bit će objavljen na oglasnoj ploči i web stranici Škole.

Predsjednica Školskog odbora:

Eni Tomšić, mag.rehab.educ.