Na temelju članka 25. stavka 2. točka 3., alineja 9. Statuta II. gimnazije, KLASA: 012-03/15-01, URBROJ: 251-97-01-15/5-03 od 16. rujna 2015., KLASA: 012-03/15-01, URBROJ: 251-97-01-15/5-05 od 19. siječnja 2016., KLASA: 012-03/16-01, URBROJ: 251-97-01-16/10-03 od 07. srpnja 2016. i KLASA: 012-03/17-01/1; URBROJ: 251-97-01/17-09 od 13. studenoga 2017., a na prijedlog ravnatelja, Školski odbor II. gimnazije na sjednici održanoj 09. ožujka 2018. godine donosi

PRAVILNIK
o sigurnoj i odgovornoj upotrebi informacijsko-komunikacijske tehnologije II. gimnazije

I. UVOD

Članak 1.

1) S obzirom na sve veću sustavnu upotrebu informacijsko-komunikacijske tehnologije (dalje u tekstu: IKT) 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.). Zbog toga je potrebno veliku pozornost posvetiti sigurnom i odgovornom korištenju IKT-a, a što je moguće postići definiranjem sigurne politike škole.
2) Svrha Pravilnika o sigurnoj i odgovornoj upotrebi informacijsko-komunikacijske tehnologije II. gimnazije (dalje u tekstu: Pravilnik) je:
   - unaprjeđenje sigurnosti školske informatičke opreme i mreže,
   - jasno i nedvosmisleno određivanje načina prihvatljivog i dopuštenog korištenja IKT resursa škole,
   - zaštita informacijskog sadržaja i opreme,
   - promoviranje sustava i usluga najprikladnijih učenicima,
   - poticanje aktivnog sudjelovanja učenika u radu s IKT-om promovirajući sigurno, odgovorno i učinkovito korištenje digitalnih tehnologija,
   - propisivanje sankcija u slučaju kršenja odredaba Pravilnika.
3) Ovaj Pravilnik primjenjuje se na sve korisnike IKT infrastrukture Škole.
4) Izrazi koji se u ovom Pravilniku koriste za osobe u muškom rodu su neutralni i odnose se na muške i ženske osobe.

Članak 2.

1) U Školi je u kolovozu 2017. godine postavljena infrastruktura CARNetove mreže. E-škole tehničarem imenovana je nastavnica informatike Smiljana Perić.
2) Učenici su dužni pridržavati se uputa koje im mogu dati nastavnici, djelatnici Škole i e- Škole tehničar, a kojima je cilj unaprjeđenje sigurnosti školske informatičke opreme i mreže.

II. OSNOVNE SIGURNOSNE ODREDBE

Članak 3.

1) Kompletna računalna mreža koja je izgrađena te računalna oprema dobivena u sklopu pilot projekta e-Škole, kao i stara računalna mreža i računalna oprema smatraju se IKT infrastrukturom Škole.
2) Korisnici IKT infrastrukture su učenici, nastavnici, ostali djelatnici i povremeni korisnici (gosti).
3) Materijalni resursi su:
   - kompletna računalna mreža izgrađena u sklopu projekta e-Škole i računalna oprema,
   - stara računalna mreža i računalna oprema.
4) Nematerijali resursi su:
   - Aplikacije koje škola koristi: e-dnevnik, e-matica, Obračun plaća s evidencijom o zaposlenicima, Meraki (središnji sustav za upravljanje računalnom mrežom).

Članak 4.

1) Školska oprema mora se čuvati i pažljivo koristiti.

Članak 5.

1) 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.
2) Tuđi osobni podaci mogu se koristiti isključivo uz prethodno odobrenje ravnatelja ili osobe koju on za to posebno opunomoći, sukladno važećim propisima koji se odnose na područje zaštite osobnih podataka.

Članak 6.

1) Računala koja su na Windows operativnim sustavima (Windows 7, 8 i 10) posjeduju antivirusni program NOD 32.
2) Učenici, nastavnici i ostali djelatnici koji se spajaju na računalnu mrežu vlastitim pametnim telefonima čiji su sustavi Android, Windows i OS, nemaju zaštitu od strane škole.
3) Na računalima u informatičkoj učionici mjera zaštite je implementirana kod davatelja internetskih usluga. Njihovi serveri blokiraju sadržaje i stranice sumnjivog karaktera .

Članak 7.

1) Djelatnici Škole posjeduju AAI@EduHr korisnički račun te su dužni koristiti službenu e-mail adresu (ime.prezime@skole.hr) za komunikaciju s nadležnim tijelima i institucijama iz sustava znanosti i obrazovanja.

Članak 8.

1) Nastavnicima i drugim djelatnicima Škole strogo je zabranjeno davati učenicima i drugim korisnicima vlastite zaporke i digitalne identitete.

Članak 9.

1) Svi djelatnici Škole moraju potpisati izjavu o tajnosti podataka te se moraju pridržavati etičkih načela pri korištenju IKT-a.

Članak 10.

1) Svako nepridržavanje ovih pravila i svako ponašanje koje nije u skladu s Pravilnikom prijavljuje se ravnatelju Škole, a sankcionirat će se temeljem važećih općih akata Škole.
2) Incidenti koji se ne mogu riješiti na razini škole prijavljuju se CARNetovom CERT-u, preko obrasca na mrežnoj stranici www.cert.hr.

III. ŠKOLSKA IKT OPREMA I ODRŽAVANJE

Članak 11.

1) Računala u školi povezana su bežično i žičano.
2) Računalna mreža se sastoji od novog dijela koje je izgrađen u sklopu pilot projekta e-Škole projekta te starog dijela mreže. U sklopu pilot projekta e-Škole imenovan je e-Škole tehničar koji je zadužen za održavanje navedene mrežne infrastrukture.
3) Računalni otpad zbrinjava se odvojeno od ostalog otpada, a Škola će takav otpad predati ovlaštenom sakupljaču EE otpada.

Članak 12.

1) Računala se bežično spajaju na 50 bežičnih pristupnih točaka. Pristupne točke su smještene u svakoj učionici, zbornici, hodnicima, kabinetima, knjižnici i čitaonici, sportskim dvoranama.
2) U bežičnim pristupnim točkama su postavljena tri naziva za pristup bežičnoj mreži (SSID):
    a) eduroam,
    b) eSkole,
    c) guest.

Članak 13.

1) Sva računala u Školi posjeduju operativni sustav Windows s instaliranim Office alatima. U informatičkoj učionici nalazi se 16 tankih klijenata s XP operacijskim sustavom koji se spajaju na server na kojem je instaliran Windows server 2012 te MS Office 2016.
2) Postavke na računalima podešene su na općenite te je na svim računalima postavljeno da kod prijave u operacijski sustav koriste zaporku. Također, uključena je opcija da lozinka nikada ne istječe (Password never expires).

3) Kod svih računala podešeno je ažuriranje operacijskog sustava i popratnih Office alata na „automatski“. Računalna mreža pokazuje da najviše prometa koja računala ostvaruju preko interneta odlazi upravo na ažuriranje navedenog.
4) Operacijski sustavi Windows 10 imaju u sebi uključen Windows Defender koji aktivno pridonosi zaštiti PC-ja tako da provjerava ima li na njemu zlonamjernog softvera, virusa i sigurnosnih prijetnji. Windows Defender koristi zaštitu u stvarnom vremenu pri pregledu svega što se preuzima i pokreće na PC-ju. Windows Update automatski preuzima ažuriranja za Windows Defender da bi PC bio siguran i zaštićen od prijetnji. Tu je i Windows vatrozid koji je dizajniran da onemogući hakerima i zlonamjernom softveru pristup na uređaj putem mreže ili interneta. Antivirusni program NOD 32 koristi se na svim računalima nabavljenim do 2016. godine.

Članak 14.

1) Škola koristi računalne programe licencirane od strane Ministarstva znanosti i obrazovanja i tvrtke Microsoft. Ministarstvo znanosti i obrazovanja izradilo je web portal Centar za preuzimanje Microsoft proizvoda. Portalu imaju pristup svi odgovorni za održavanje i instalaciju računalnih programa u školama (administratori sustava).
2) U sustav se prijavljuje AAI@EduHr korisničkim računom gdje se mogu preuzeti svi navedeni operacijski sustavi i Office alati s pripadajućim ključevima za aktivaciju.
3) Svi računalni programi moraju se koristiti u skladu s propisima i pripadajućim licencama.

Članak 15.

1) Učenici ne smiju instalirati nikakve računalne programe u informatičkoj učionici (igrice ili sl.).
2) Na ostala računala u Školi nije dopušteno ništa instalirati bez odobrenja administratora. Ako postoji potreba za instaliranjem dodatnog računalnog programa, djelatnik odnosno učenik koji ga želi instalirati dužan je obvezno se javiti administratoru.

Članak 16.

1) Svako nepridržavanje ovih pravila može rezultirati disciplinskim mjerama prema djelatnicima Škole ili pedagoškim mjerama prema učenicima.

IV. REGULIRANJE PRISTUPA IKT OPREMI

Članak 17.

1) Računalnoj mreži mogu pristupiti učenici, nastavnici, ostali djelatnici škole te vanjski partneri i posjetitelji.
2) Pristup bežičnoj računalnoj mreži zaštićen je na nekoliko načina. Pristup ovisi o tome tko se želi spojiti na mrežu i s kojim razlogom.
3) U bežičnim pristupnim točkama su postavljene 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.

b) eSkole mreža se koristiti za spajanje uređaja u STEM učionicama gdje se učenici i nastavnici 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.

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 omogućen je pristup na eduroam mrežu uz ograničenje brzine pristupa. Ostalim partnerima i posjetiteljima može se 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. Brzina ove mreže je ograničena na 10% ukupne brzine internetske veze.

4) U sklopu projekta e-Škole, nastavnici i stručni suradnici zaduženi su opremom (hibridna računala, tableti i prijenosna računala).
5) U slučaju duže odsutnosti djelatnika, a u svrhu normalnog funkcioniranja nastavnog procesa, djelatnik je dužan vratiti opremu, o čemu odluku donosi ravnatelj.

Članak 18.

1) Učenici smiju uz dopuštenje nastavnika koristiti samo školska računala koja su njima namijenjena (računala u informatičkoj učionici i u STEM učionicama).
1) Vlastita računala i pametne telefone učenici smiju za vrijeme nastave koristiti isključivo u obrazovne svrhe i uz prethodno dopuštenje nastavnika, 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 nastavnik.
2) Učenici smiju koristiti vlastita računala u privatne svrhe isključivo za vrijeme odmora te prije i poslije nastave.

Članak 19.

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

Članak 20.

1) Svi nastavnici koji koriste informatičku i STEM učionice moraju se pridržavati sljedećih naputaka:
   - učionica mora ostati na kraju onako kako je i zatečena,
   - računala se obavezno moraju isključiti nakon uporabe,
   - u slučaju da neko od računala ne radi treba kontaktirati nastavnika informatike (voditelja informatičke učionice),
   - radna mjesta moraju ostati uredna (namještena tipkovnica, miš, monitor, stolica na svojem mjestu),
   - prozore obavezno zatvoriti,

– učionicu zaključati.

2) Nastavnik informatike (voditelj informatičke učionice) odgovoran je za informatičku učionicu.

Članak 21.

1) U Školi su sva računala podešena tako da se za ulaz u operativni sustav koristi zaporka. Također je uključena opcija u operativnom sustavu da loznika nikada ne prestaje (Password never expires).
2) Preporučuje se korištenje korisničkih zaporki koje se sastoje od kombinacije malih i velikih slova, brojeva i posebnih znakova te su minimalne duljine 6 znakova.

Članak 22.

1) Odlukom Ministarstva znanosti i obrazovanja sve osnovne i srednje škole spojene na CARNet mrežu automatski su uključene i u sustav filtriranja nepoćudnih sadržaja.
2) 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.
3) Ako učenik smatra da je određeni sadržaj neopravdano blokiran ili propušten može se obratiti nastavniku informatike.
4) Ako učenici primjete neprimjerene, uznemirujuće ili sadržaje koji ugrožavaju njihovu sigurnost, o tome odmah trebaju obavijestiti nastavnike ili ravnatelja.
5) U Školi postoji nadzor mrežnog prometa kroz Meraki Cloud System od strane e-Škole tehničara.

V. SIGURNOST KORISNIKA

Članak 23.

1) U Školi je potreba neprekidna edukacija učenika, nastavnika i ostalih djelatnika da bi se mogao održati korak u korištenju IKT-a, kao i s nadolazećim prijetnjama u računalnoj sigurnosti.
2) Prigodom korištenja računala i programi koji zahtijevaju prijavu lozinkom, potrebno je voditi računa da se kod prijave ne otkriju podaci o prijavi.
3) Kada učenici odlaze iz učionice, a ostavljaju računalo uključeno, nastavnici su dužni odjaviti ih iz svih sustava u koje su se prijavili.
4) Također, učenici koji koriste računala u STEM učionicama, dužni su se obvezno nakon završetka rada odjaviti iz sustava u koje su se prijavili.

Članak 24.

1) Korisnici su dužni posebno voditi računa o svojem elektroničkom identitetu koji su dobili iz sustava AAI@edu. Svoje podatke moraju čuvati.
2) Početkom školovanja u Školi svi učenici dobivaju elektronički identitet u sustavu AAI@EduHr.

3) U slučaju gubitka korisničke oznake ili zaporke, odnosno u slučaju kada je učeniku zaključan elektronički identitet, učenik se treba javiti administratoru imenika.
4) Kada učenik prelazi u Školu iz druge škole, njegov elektronički identitet se prenosi.
5) Minimalno jednom godišnje (početkom školske godine) potrebno je revidirati elektroničke identitete učenika.
6) Nakon isteka učeničkog statusa i prestanka potrebe za posjedovanjem elektroničkog identiteta učenika, identitet je potrebno isključiti.
7) Pri zapošljavanju novog djelatnika, administrator imenika dodjeljuje mu elektronički identitet u sustavu AAI@EduHr, a pri prestanku radnog odnosa, identitet je potrebno isključiti.
8) Pravila pristupa učenika i djelatnika Škole školskim računalima potrebno je redovito provjeravati i po potrebi mijenjati.

Članak 25.

1) Datoteke preuzete iz nekog vanjskog izvora (putem elektroničke pošte, vanjskog diska ili interneta) mogu ugroziti sigurnost učenika odnosno nastavnika te je pravilo ne otvarati ili prosljeđivati zaražene datoteke i programe. Također, pravilo je ne otvarati datoteke iz sumnjivih ili nepoznatih izvora.
2) Sve nepoznate i sumnjive datoteke potrebno je provjeriti antivirusnim alatom prije korištenja.

VI. PRIHVATLJIVO I ODGOVORNO KORIŠTENJE INFORMACIJSKO-KOMUNIKACIJSKE TEHNOLOGIJE

Ponašanje na internetu

Članak 26.

1) 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.
2) Škola će korisnike upoznati s pravilima poželjnog ponašanja na internetu - „Netiquette“, objavljivanjem navedenih pravila u informatičkoj učionici.

Članak 27.

1) Učenike se na nastavi informatike i satu razredne zajednice 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...).

Članak 28.

1) 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).

Autorsko pravo

Članak 29.

1) Korisnike se potiče da potpisuju materijale koje su sami izradili, ali i da poštuju tuđe radove. Nipošto ne smiju tuđe radove predstavljati kao svoje, preuzimati zasluge za tuđe radove, niti nedozvoljeno preuzimati tuđe radove s interneta.
2) Korištenje tuđih materijala s interneta mora biti citirano, obavezno navodeći autora korištenih materijala te izvor informacije (poveznica i datum preuzimanja).

Članak 30.

1) Računalni programi su također zaštićeni zakonom kao jezična djela. Najčešće su zaštićeni samo izvorni programi, ali ne i ideje na kojima se oni zasnivaju, a u što su uključeni i on-line programi odnosno web aplikacije.

Članak 31.

1) 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 32.

1) Pri korištenju digitalnih sadržaja, a osobito pri njihovu dijeljenju treba biti osobito oprezan.
2) U Školi je izričito zabranjeno nelegalno dijeljenje datoteka (npr. kopiranje ili preuzimanje autorski zaštićenog materijala poput e-knjige, glazbe ili pak videosadržaja).
3) Učenike i nastavnike treba podučiti o autorskom pravu i intelektualnom vlasništvu te ih usmjeriti na korištenje licenci za zaštitu autorskog prava i intelektualnog vlasništva.
4) Učenike i nastavnike treba podučiti o načinima nelegalnog dijeljenja datoteka i servisima koji to omogućuju (npr. Torrent).
5) Učenike i nastavnike treba informirati o mogućim posljedicama nelegalnog korištenja, dijeljenja i umnažanja autorski zaštićenih materijala.

Internetsko nasilje

Članak 33.

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

2) 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.

Članak 34.

1) Potrebno je učenike i nastavnike educirati o mogućim oblicima internetskog nasilja te o tome kako prepoznati internetsko nasilje.
2) U Školi je potrebno razviti nultu stopu tolerancije na internetsko nasilje.
3) Nedopušteni su svi oblici nasilničkog ponašanja te će svi oni za koje se utvrdi da provode takve aktivnosti disciplinski odgovarati.

Korištenje mobilnih telefona

Članak 35.

1) Kućnim redom Škole zabranjeno je korištenje mobilnih telefona za vrijeme nastave.
2) Iznimno, učenici mogu koristiti mobilne telefone za vrijeme nastave, kada nastavnik to zatraži i pravovremeno najavi.
3) Učenici mogu u Školi koristiti mobilne telefone za vrijeme odmora, prije ili poslije nastave, poštujući odredbe Kućnog reda Škole i ovoga Pravilnika.
4) S obzirom da mobilni telefoni sve više imaju potpuni pristup internetu te da djeca i mladi koriste fiksne internetske veze kao i mobitele 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 slično).
5) Škola će upoznati učenike s posljedicama zlouporabe mobilnih telefona. Najrašireniji oblik nasilja među vršnjacima je nasilje putem mobilnih telefona koje uključuje bilo kakav oblik poruke zbog koje se osoba osjeća neugodno ili joj se tako prijeti (tekstualna poruka, videoporuka, fotografija, poziv), odnosno kojoj je cilj uvrijediti, zaprijetiti, nanijeti bilo kakvu štetu vlasniku mobilnog telefona.

Članak 36.

1) Ovaj Pravilnik stupa na snagu danom donošenja te se objavljuje na oglasnoj ploči škole.

KLASA: 021-04/18-01
URBROJ: 251-97-01/18-03-01/1
Zagreb, 09. ožujka 2018.

PREDSJEDNICA ŠKOLSKOG ODBORA	RAVNATELJ
_____	_____
Irena Ihas Jurić, prof.,v.r.	Drago Bagić, prof.,v.r.