Gimnazija Sesvete
Bistrička 7
10360 Sesvete

PRAVILNIK O SIGURNOJ I ODGOVORNOJ UPOTREBI INFORMACIJSKO-KOMUNIKACIJSKE TEHNOLOGIJE

GIMNAZIJE SESVETE

Zagreb, 2018.

Na temelju članka 25. stavka 2. točka 3. Statuta Gimnazije Sesvete KLASA:602-03/15-05/14, URBROJ:251-116-15-07 od 8.rujna 2015. godine, KLASA:602-03/15-05/25 URBROJ: 251-116-15-07 od 30. prosinca 2015. godine., KLASA: 602-03/16-05/9 URBROJ: 251-116-16-07 od 5. srpnja 2016. godine, KLASA : 602-03/17-05/34 , URBROJ: 251-116-17-07 od 10. studenog 2017. te članka 118. Zakona o odgoju i obrazovanju u osnovnoj i srednjoj školi (NN 87/08,86/09,92/10,105/10,5/12,16/12,86/12,126/12,94/13,152/14 i 07/17.) Školski odbor Gimnazije Sesvete, na prijedlog ravnatelja, na sjednici održanoj19. veljače 2018. godine donosi

PRAVILNIK O SIGURNOJ I ODGOVORNOJ UPOTREBI INFORMACIJSKO-KOMUNIKACIJSKE TEHNOLOGIJE GIMNAZIJE SESVETE

I. UVOD

Članak 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 sigurnosne politike škole.

Svrha Pravilnika o sigurnoj i odgovornoj upotrebi informacijsko-komunikacijske tehnologije Gimnazije Sesvete (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 kazni u slučaju kršenja odredaba Pravilnika.

Ovaj Pravilnik primjenjuje se na sve korisnike IKT infrastrukture Škole.

Članak 2.

U školi je u kolovozu 2017. godine postavljena infrastruktura CARNetove mreže. Škola ima tehničara za projekt e-škole.

Članak 3.

Učenici su dužni pridržavati se uputa koje im daju djelatnici Škole i e- škole tehničar, a kojima je cilj unaprjeđenje sigurnosti školske informatičke opreme i mreže.

Svi školski djelatnici dužni su se pridržavati uputa koje im daje ovlaštena osoba radi unaprjeđenja sigurnosti školske informatičke opreme i mreže.

II. OSNOVNE SIGURNOSNE ODREDBE

Članak 4.

U sklopu pilot projekta e-Škole izgrađena je računalna WiFi mreža i dobivena je računalna oprema. Spomenuta WiFi mreža i računalna oprema zajedno sa starom žičanom računalnom mrežom i računalnom opremom čini IKT infrastrukturu Škole.

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

Materijalni resursi su:

- kompletna računalna mreža izgrađena u sklopu projekta e-Škole i računalna oprema
- već ranije postavljena računalna mreža i računalna oprema.

Nematerijalni resursi su:

- aplikacije koje škola koristi odobrenjem nadležnih institucija.

Članak 5.

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

Školska se oprema mora čuvati i pažljivo koristiti. Korisnici ne smiju uništavati IKT infrastrukturu škole. Svaki radnik pri preuzimanju opreme na korištenje potpisuje zadužnicu kojom se obvezuje po prestanku korištenja vratiti opremu u ispravnom stanju, a u suprotnom odgovara za nastalu štetu.

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

Članak 6.

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 (kontaktni 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. kontaktni podaci osobe, fotografije osobe i sl.), podaci iz evidencija koje vodi Škola (e-Dnevnik, e-Matica, matične knjige i sl.) te informacije koje se smatraju poslovnom tajnom.

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

Članak 7.

Sva računala koriste Windows operativni sustav. Za zaštitu od zlonamjernih programa operativnih sustava koristi se antivirusni program.

Učenici, nastavnici i ostali djelatnici koji se spajaju na računalnu mrežu vlastitim pametnim telefonima čiji su sustavi Android, Windows i OS i sl. nemaju zaštitu od škole.

Davatelj internetskih usluga implementirao je mjere zaštite na računalima u učionicama. Njihovi serveri blokiraju sadržaje i stranice sumnjivog karaktera.

Članak 8.

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

Članak 9.

Strogo se zabranjuje davati drugim osobama vlastite zaporke i digitalne identitete.

Članak 10.

Svi djelatnici Škole koji zbog prirode posla imaju pristup osobnim podacima ostalih osoba dužni su se pridržavati važećih propisa i etičkih načela iz područja zaštite osobnih podataka i pri korištenju IKT-a. Na zahtjev Škole moraju potpisati izjavu o tajnosti podataka.

Članak 11.

Svako nepridržavanje ovih pravila i svako ponašanje koje nije u skladu s Pravilnikom prijavljuje se ravnatelju Škole, a kaznit će se temeljem važećih općih akata Škole.

Ozbiljniji incidenti prijavljuju se CARNetovom CERT-u putem obrasca na mrežnoj stranici www.cert.hr.

III. ŠKOLSKA IKT OPREMA I ODRŽAVANJE

Članak 12.

Računala su u školi povezana bežično i žičano. Računalna se mreža sastoji od novog dijela koji je izgrađen u sklopu pilot projekta e-Škole (bežična mreža) te starog dijela mreže (žičana mreža). U sklopu pilot projekta e-Škole imenovan je tehničar e-Škole koji je zadužen za održavanje navedene mrežne infrastrukture.

Članak 13.

Računalni otpad zbrinjava se odvojeno od ostalog otpada, a Škola će takav otpad predati ovlaštenom sakupljaču EE otpada.

Članak 14.

Računala se bežično spajaju na pristupne točke. Bežične pristupne točke smještene su u svakoj učionici, zbornici, holu, uredima i sportskoj dvorani. U bežičnim su pristupnim točkama postavljena tri naziva za pristup bežičnoj mreži (SSID):

a) eduroam

b) eSkoleeSkole

c) guest.

Članak 15.

Sva računala u Školi posjeduju operativni sustav Windows s instaliranim Office alatima. Postavke su na računalima postavljene na općenite, a na svim računalima koristi se zaporka prilikom prijave u operativni sustav. Uključena je opcija da lozinka nikada ne ističe (Password never expires). Na svim računalima ažurira se automatski operativni sustav i popratni Office alat.

Operativni sustavi Windows 10 imaju u sebi obrambeni sustav (Windows Defender Security Center) te i vatrozid.

Članak 16.

Škola koristi računalne programe licencirane od 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).

U sustav se prijavljuje AAI@edu korisničkim računom gdje se mogu preuzeti svi navedeni operativni sustavi i office alati s pripadajućim ključevima za aktivaciju.

Svi programi koji su instalirani i korišteni na uređajima moraju imati važeću licencu te se moraju upotrebljavati u skladu s važećim propisima i pripadajućim licencama. Ako se netko koristi nelegalnim softverom ili softverom koji je instalirao bez dopuštenja, osobno snosi posljedice, a osoba odgovorna za održavanje opreme nije dužna popraviti štetu koja je nastala upotrebom neovlaštenog instaliranog softvera.

Za sva računala i programe koji su dodijeljeni nastavnicima u sklopu projekta e-Škole odgovorne su isključivo zadužene osobe, kao i za programe na školskim računalima jer svi programi koji se instaliraju i koriste moraju imati važeću licencu te se moraju upotrebljavati u skladu s važećim propisima i licencama.

Članak 17.

Učenici ne smiju instalirati nikakve računalne programe u učionicama (igrice ili sl.).

Na ostala računala u Školi nije dopušteno ništa instalirati bez odobrenja administratora. Ako se pojavi potreba za instaliranjem dodatnog računalnog programa, djelatnik, odnosno učenik koji ga želi instalirati mora se obvezno javiti administratoru.

Članak 18.

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

IV. REGULIRANJE PRISTUPA IKT OPREMI

Članak 19.

Računalnoj žičanoj mreži mogu pristupiti učenici, nastavnici, ostali djelatnici škole te vanjski partneri i posjetitelji.

Pristup bežičnoj računalnoj mreži zaštićen je na nekoliko načina. Pristup ovisi o tome tko se želi spojiti na mrežu i s kojim razlogom.

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

a) eduroameduroam

b) eSkoleeSkole

c) guest.

a) Na eduroam mrežu spajaju se nastavnici i učenici sa svojim privatnim ili školskim uređajima.

b) eSkole mreža koristiti se 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 se način može identificirati i pratiti njihov promet u računalnoj mreži.

c) Guest mreža koristi se 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 može se na zahtjev omogućiti pristup bežičnoj mreži. Bežična mreža guest je otvorenog tipa, a za autentikaciju koristi se Captive portal. Kako bi im se omogućio pristup, tehničar e-Škole mora u Meraki dashboardu kreirati korisničko ime za svakog korisnika kojem škola odobri pristup mreži.

Članak 20.

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

Vlastita računala i pametne telefone učenici smiju za vrijeme nastave koristiti isključivo u obrazovne svrhe i uz prethodnu dozvolu nastavnika pri čemu moraju paziti da ne ugrožavaju druge korisnike školske mreže širenjem virusa i drugih zlonamjernih programa. Nastavnik određuje kojim aplikacijama i internetskim sadržajima mogu pristupiti učenici.

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

Učenici su dužni svaki uočeni kvar (hardverski ili softverski) prijaviti nastavniku te ne smiju samovoljno popravljati računala.

Članak 21.

Osim računalima koja su dobili u sklopu pilot projekta e-Škole nastavnici imaju pristup računalima u zbornici, knjižnici i u drugim prostorijama Škole, a ostalo osoblje računalima u uredima Škole.

Članak 22.

Svi nastavnici koji koriste računalnu opremu u učionicama moraju se pridržavati sljedećih naputaka:

- Učionica se mora ostaviti uredno na kraju nastave.
- Računala se obavezno moraju ugasiti nakon uporabe.
- U slučaju da neko računalo ne radi treba kontaktirati nadležnu osobu.
- Radna mjesta moraju ostati uredna (namještena tipkovnica, miš, monitor, stolica na svojem mjestu).
- Prozore obavezno zatvoriti.
- Učionicu zaključati.

Nastavnik (korisnik učionice) odgovoran je za učionicu.

Članak 23.

U Školi su sva računala postavljena tako da se koristi zaporka za ulaz u operativni sustav 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 šest znakova.

Članak 24.

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 nastavniku. Ako učenici primijete neprimjerene, uznemirujuće ili sadržaje koji ugrožavaju njihovu sigurnost, o tome odmah trebaju obavijestiti nastavnike ili ravnatelja.

Tehničar e-Škole nadzire bežični mrežni promet kroz Meraki Cloud System.

V. SIGURNOST KORISNIKA

Članak 25.

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

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

Članak 26.

Korisnici su dužni posebno voditi računa o svojem elektroničkom identitetu koji su dobili iz sustava AAI@edu. 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, učenik se treba javiti administratoru imenika. Kada učenik prelazi u Školu iz druge škole, njegov elektronički se identitet prenosi.

Elektroničke identitete učenika potrebno je revidirati prema potrebi.

Učenički identitet potrebno je isključiti nakon isteka učeničkog statusa i prestanka potrebe za posjedovanjem elektroničkog identiteta učenika.

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

Članak 27.

Datoteke preuzete iz nekog vanjskog izvora (putem elektroničke pošte, vanjskog diska, ili interneta) mogu ugroziti sigurnost učenika, odnosno nastavnika. Zaražene datoteke i programe uputno je ne otvarati ili prosljeđivati, kao i datoteke iz sumnjivih ili nepoznatih izvora. Prije korištenja potrebno je sve takve datoteke provjeriti antivirusnim alatom.

VI. PRIHVATLJIVO I ODGOVORNO KORIŠTENJE INFORMACIJSKO-KOMUNIKACIJSKE TEHNOLOGIJE

Ponašanje na internetu

Članak 28.

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

Škola će korisnike upoznati s pravilima poželjnog ponašanja na internetu, odnosno mrežnog bontona objavljivanjem navedenih pravila u Školi.

Članak 29.

Učenike se na nastavi i na satu razrednog odjela 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 i sl.).

Članak 30.

Osim Pravila poželjnog ponašanja na internetu uputno je da se učenici pridržavaju i sljedećih naputaka (Pravila sigurnog ponašanja):

- Osobne se informacije na internetu nikad ne smiju odavati.
- Zaporka je tajna i nikad se ne smije nikome reći.
- Uočeno bilo kakvo zlostavljanje potrebno je odmah prijaviti nadležnim osobama i/ili institucijama.
- Treba provjeriti jesu li zaštićeni osobni podaci na društvenim mrežama.
- Fotografiranje i snimanje osoba smije se napraviti samo uz prethodno dopuštenje. Potrebno je imati i dopuštenje za objavu takvih digitalnih sadržaja.
- Potrebno je biti oprezan s objavljivanjem sadržaja na društvenim mrežama.

- Treba provjeriti postoji li neka mrežna stranica o nama te koje informacije sadrži (treba upisati svoje ime i prezime u Google).

Autorsko pravo

Članak 31.

Korisnike se potiče da potpisuju materijale/radove koje su sami izradili, ali i da poštuju materijale/radove drugih. Ne smije se materijale/radove drugih predstavljati kao svoje, preuzimati zasluge za iste i preuzimati ih s interneta. Korištenje materijala/radova s interneta mora biti citirano uz obavezno navođenje autora korištenih materijala/radova te izvora informacije (poveznica i datum preuzimanja).

Članak 32.

Sav sadržaj koji je dostupan na internetu podliježe Zakonu o autorskim pravima i srodnim zakonima i pravilnicima. Računalni su programi također zaštićeni zakonom kao jezična djela. Najčešće su zaštićeni samo izvorni programi, no ne i ideje na kojima se oni zasnivaju, a u što su uključeni i on-line programi, odnosno web aplikacije.

Članak 33.

Na mrežnim mjestima moguće je posebno zaštititi samo objavljeni sadržaj, ali 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 34.

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 videosadržaja).

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.

Internetsko nasilje

Članak 35.

Internetsko se nasilje općenito definira kao namjerno i ponovljeno 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 internetu
- lažno predstavljanje žrtve na internetu
- slanje prijetećih poruka, uznemirujućih fotografija, videa i ostalih sadržaja
- postavljanje internetske ankete o žrtvi
- slanje virusa na e-mail ili mobitel
- i ostali oblici koji nisu navedeni u ovom članku.

Članak 36.

Nedopušteni su svi oblici internetskog nasilja te će disciplinski odgovarati svi oni za koje se utvrdi da provode takve aktivnosti.

Svi korisnici, ovisno o težini povrede, odgovaraju za internetsko nasilje koje su počinili. Škola može učenicima izreći pedagošku mjeru u skladu s propisima koji uređuju izricanje pedagoških mjera, a djelatnicima upozorenje na obveze iz radnog odnosa u skladu s propisima radnog prava.

Korištenje mobilnih telefona

Članak 37.

Zabranjeno je korištenje mobilnih telefona za vrijeme nastave.

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

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

Škola će upoznati učenike s posljedicama zlouporabe mobilnih telefona.

Članak 38.

Ovaj Pravilnik stupa na snagu danom donošenja.

KLASA:602-03/18-05/13
URBROJ:251-116-18-05
Zagreb, 19.veljače 2018.

PREDSJEDNICA ŠKOLSKOG ODBORA

_____

SONJA BATINIĆ, prof.