



KRAPINSKO-ZAGORSKA ŽUPANIJA

Gimnazija **Antuna Gustava Matoša** Zabok

Na temelju članka 56. Statuta Gimnazije Antuna Gustava Matoša, (KLASA: 012-03/19-01/01, URBROJ: 2197/01-380/1-6-19-10 od 2. srpnja 2019.) i članka 118. Zakona o odgoju i obrazovanju u osnovnoj i srednjoj školi (NN br. 87/08, 86/09, 92/10, 105/10, 90/11, 5/12, 16/12, 86/12, 94/13, 152/14, 7/17, 68/18, 98/19, 64/20, 133/20), Školski odbor Gimnazije Antuna Gustava Matoša – Zabok (u daljnjem tekstu: Škola), Prilaz Janka Tomića 2, 49210 Zabok, na 31. sjednici održanoj 21. prosinca 2022. godine donosi:

PRAVILNIK

o sigurnoj i odgovornoj upotrebi informacijsko-komunikacijske tehnologije Gimnazije Antuna Gustava Matoša

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 sustavu škole 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.

Svrha Pravilnika o sigurnoj i odgovornoj upotrebi informacijsko-komunikacijske tehnologije 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.

Ovaj Pravilnik primjenjuje se na sve korisnike IKT infrastrukture Škole.

Izrazi koji se u ovom Pravilniku koriste za osobe u muškom rodu su neutralni i odnose se na muške i ženske osobe.

Članak 2.

U Školi je u kolovozu 2018. godine postavljena infrastruktura CARNetove mreže. Tehničarem E-škole imenovan je nastavnik informatike Mihael Bobičanec.

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.

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.

- 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,
- stara računalna mreža i računalna oprema.

Nematerijalni resursi su:

- Aplikacije koje škola koristi: e-dnevnik, e-matica, e-upisi, e-matura, e-natjecanja, EMA, Carnet Loomen, Edupage, ASC raspored, Office online, Obračun plaća s evidencijom o zaposlenicima...

Članak 4.

Školska oprema mora se 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.

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.

Računala koja su na Windows operativnim sustavima posjeduju njegov osnovni antivirusni program.

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

Na računalima u informatičkoj učionici mjera zaštite je implementirana kod davatelja internetskih usluga. Njihovi serveri blokiraju sadržaje i stranice sumnjivog karaktera .

Članak 7.

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.

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

Članak 9.

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

Članak 10.

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.

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.

Računala u školi povezana su bežično i žičano.

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.

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

Članak 12.

Računala se bežično spajaju na bežičnu pristupnu točku. Pristupna točka je dostupna u svakoj učionici, zbornici, hodnicima, kabinetima, knjižnici i čitaonici.

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

- eduroam,
- eSkole,
- guest.

Članak 13.

Sva računala u Školi posjeduju operativni sustav Windows s instaliranim Office alatima. U informatičkoj učionici nalazi se 25 računala s operacijskim sustavom Windows te MS Office 2016.

Kod svih računala podešeno je ažuriranje operacijskog sustava i popratnih Office alata na „automatski“.

Operacijski sustavi Windows imaju u sebi uključen antivirusni program koji aktivno pridonosi zaštiti PC-ja tako da provjerava ima li na njemu zlonamjernog softvera, virusa i sigurnosnih prijetnji. Antivirusni program koristi zaštitu u stvarnom vremenu pri pregledu svega što se preuzima i pokreće na PC-ju. Windows Update automatski preuzima ažuriranja za antivirusni program 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.

Članak 14.

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. Pristup portalu imaju svi odgovorni za održavanje i instalaciju računalnih programa u školama (administratori sustava).

U sustav se prijavljuje AAI@EduHr korisničkim računom gdje se mogu preuzeti svi dostupni operacijski sustavi i Office alati s pripadajućim ključevima za aktivaciju.

Svi računalni programi moraju se koristiti u skladu s propisima i pripadajućim licencama.

Članak 15.

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

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 javiti se administratoru.

Članak 16.

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

IV. REGULIRANJE PRISTUPA IKT OPREMI

Članak 17.

Računalnoj 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.

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

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.

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.

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

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

Korištenje vlastitih prijenosnih računala

Članak 18.

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

Kućnim redom Škole zabranjeno je korištenje vlastitih prijenosnih računala (pametnih telefona, tableta i ostalih vrsta prijenosnih računala) za vrijeme nastave. Učenici smiju vlastita prijenosna računala 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.

Iznimno, učenici mogu koristiti vlastita prijenosna računala za vrijeme nastave, kada nastavnik to zatraži i pravovremeno najavi.

Učenici smiju koristiti vlastita prijenosna računala u privatne svrhe isključivo za vrijeme odmora te prije i poslije nastave, poštujući odredbe Kućnog reda Škole i ovoga Pravilnika.

Članak 19.

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

Članak 20.

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

- učionica mora ostati u istom stanju 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.

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

Članak 21.

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 informatike.

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.

V. SIGURNOST KORISNIKA

Članak 22.

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.

Prigodom 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.

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

Članak 23.

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 kada je učeniku zaključan elektronički identitet, učenik se treba javiti administratoru imenika.

Kada učenik prelazi u Školu iz druge škole, njegov elektronički identitet se prenosi.

Minimalno jednom godišnje (početkom školske godine) potrebno je revidirati elektroničke identitete učenika.

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

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

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

Članak 24.

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.

Sve nepoznate i sumnjive datoteke potrebno je provjeriti antivirusnim alatom prije korištenja.

VI. PRIHVATLJIVO I ODGOVORNO KORIŠTENJE INFORMACIJSKO-KOMUNIKACIJSKE TEHNOLOGIJE

Ponašanje na internetu

Članak 25.

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 objavljivanjem navedenih pravila u informatičkoj učionici.

Članak 26.

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 27.

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 odgovarati 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.
- 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).

Odgovornost za sadržaje

Članak 28.

Učenike se upozorava da se prilikom korištenja i objavljivanja na Internetu moraju znati da su odgovorni za sve što pišu, objavljuju i komentiraju na Internetu. Njihova privatna aktivnost ovdje se također uzima u obzir.

Znanje o publici

Članak 29.

Uputno je da svatko tko objavljuje sadržaje kroz društvene mreže i medije vodi brigu o publici koja će to čitati.

Mogući posjetitelji mogu biti školski kolege, potencijalni poslodavci, suradnici, učitelji i slično.

Razumijevanje koncepta zajednice

Članak 30.

Budući da društvene zajednice na internetu postoje kako bi se njihovi članovi mogli međusobno podržavati, svaki korisnik mora dobro balansirati između privatnih i školskih informacija koje dijeli s drugima.

Korisnici ne smiju poticati suparništvo, već suradnju i međusobno pomaganje.

Autorsko pravo

Članak 31.

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.

Korištenje tuđih materijala s interneta mora biti citirano, obavezno navodeći autora korištenih materijala te izvor informacije (poveznica i datum preuzimanja).

Članak 32.

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 33.

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 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 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.

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

Internetsko nasilje

Članak 35.

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

Najrašireniji oblik nasilja među vršnjacima je nasilje putem elektroničkih uređaja koje uključuje bilo kakav oblik poruke zbog koje se osoba osjeća neugodno ili joj se tako prijeti (tekstualna poruka, video-poruka, fotografija, poziv), odnosno kojoj je cilj uvrijediti, zaprijetiti ili nanijeti bilo kakvu štetu žrtvi.

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 36.

Potrebno je učenike i nastavnike educirati o mogućim oblicima internetskog nasilja, posljedicama zlorabe mobilnih telefona te o tome kako prepoznati internetsko nasilje.

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

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

Članak 37.

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

KLASA: 003-05/22-01/05

URBROJ: 2140-91/01-22-1

Zabok, 21. prosinca 2022.

PREDSJEDNICA ŠKOLSKOG ODBORA

Novački Maja

Maja Novački, prof.



PRAVNATELJICA

Šlogar Bibijana

Bibijana Šlogar, prof.

