



Republika Hrvatska
XV. gimnazija
IB World School
Zagreb, Jordanovac 8



Na temelju članka 29., stavka 2., točke 3., alineje 9. Statuta XV. gimnazije, KLASA: 012-03/15-01/01, URBROJ: 251-94-08-15-1 od 4. rujna 2015., KLASA: 003-06/15-01/39, URBROJ: 251-94-08-15-3 od 10. prosinca 2015., KLASA: 003-06/16-01/19, URBROJ: 251-94-08-16-10 od 6. srpnja 2016. KLASA: 012-03/17-01/03, URBROJ: 251-94-08-17-4 od 10. listopada 2017. godine, na prijedlog ravnateljice Školski odbor na 11. sjednici održanoj dana 11. prosinca 2017. godine donosi

ODLUKU O PRIHVATLJIVOM KORIŠTENJU RAČUNALNIH RESURSA XV. GIMNAZIJE

OSNOVNE ODREDBE

I.

- (1) Odlukom o prihvatljivom korištenju računalnih resursa XV. gimnazije (dalje: Odluka) uređuju se osnovne sigurnosne odredbe, informacijsko-komunikacijska tehnologija (dalje: IKT) i njezino održavanje te uvjeti prihvatljivog i odgovornog korištenja IKT opreme XV. gimnazije.
- (2) Svrha je ove Odluke jasno određivanje načina dopuštenog i prihvatljivog korištenja računalnih resursa XV. gimnazije (dalje: škola).
- (3) Cilj je ove Odluke povećanje sigurnosti rada i učenja u školi.

OPĆE SIGURNOSNE ODREDBE

Korisnici

II.

- (1) Korisnici računalnih resursa škole jesu radnici, učenici, vanjski suradnici za održavanje i svaka druga osoba koja uz odobrenje škole koristi računalne resurse škole.
- (2) Radnici se moraju pridržavati uputa koje im daju školski administratori sustava ili druge ovlaštene osobe. Učenici se moraju pridržavati uputa koje im daju nastavnici ili druge ovlaštene osobe. Vanjski korisnici i druge osobe dužne su postupati po uputama ovlaštene osobe radi unapređenja sigurnosti školske informatičke opreme i mreže. Svi korisnici dužni su, prilikom korištenja računalnih resursa škole, pridržavati se odredbi Odluke te drugih primjenjivih propisa.

(3) Svako nepridržavanje ovih pravila ima negativan utjecaj za školu i može rezultirati disciplinskim mjerama prema radnicima ili pedagoškim mjerama prema učenicima, odnosno pokretanjem odgovarajućih postupaka prema trećim osobama u skladu s važećim propisima.

(4) Obveza je škole osigurati da se na području njezine odgovornosti korisnici ponašaju u skladu s odredbama Odluke o prihvatljivom korištenju CARNet mreže.

(5) Svatko je dužan ponašanje protivno ovoj Odluci prijaviti odgovornoj osobi (nastavniku, administratoru resursa, administratoru imenika, sistem inženjeru mreže, voditelju informatičkih učionica ili ravnatelju).

IKT infrastruktura

III.

(1) IKT infrastrukturu škole čine fiksna i bežična mreža sa svim svojim mrežnim uređajima, sva školska stolna, prijenosna i tablet računala, školski mobilni telefoni te ulazno-izlazni uređaji bez obzira na to jesu li vlasništvo škole ili se škola služi tim uređajima.

(2) IKT infrastruktura mora omogućavati neometan pristup i korištenje informacijama potrebnih u nastavi i drugim aktivnostima vezanim za rad škole.

(3) 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.

Sigurnost informacija

IV.

(1) Načelo povjerljivosti informacija podrazumijeva da informacije moraju biti dostupne samo onome kome su namijenjene. Škola razlikuje javne i interne informacije.

(2) Skupinu javnih informacija čine informacije koje opisuju djelatnosti škole, a njihova je javna dostupnost u interesu škole, kao na primjer sadržaji i podaci koje je škola dužna objavljivati na svojim mrežnim stranicama, informacije o aktivnostima škole i slično.

(3) Skupinu internih informacija čine informacije koje se odnose na osobne podatke pojedinaca (npr. kontakt podaci osobe, fotografije osobe, podaci iz pedagoške evidencije i evidencije o radnicima koje vodi škola) informacije koje su namijenjene samo djelatnicima škole. Zabranjeno je koristiti se tuđim osobnim podacima bez dopuštenja osobe odgovorne za te podatke.

(4) Dokumentacija škole čuva se na zakonom i drugim propisima određeni način, ovisno o vrsti gradiva.

(5) Sigurnosna je preslika kopija podataka na drugom mediju za pohranu podataka, redovito se izrađuje za sve podatke koji se pohranjuju na računalima škole za koje škola procijeni da su važni. Odgovorne osobe dužne su raditi redovite sigurnosne preslike za te podatke. Svaki je radnik odgovoran za izrađivanje sigurnosnih preslika svojih podataka.

(6) Mjere fizičke sigurnosti primjenjuju se na sva mjesta gdje se nalaze podaci važni za rad škole, uz primjenu važećih propisa, tehničkih pravila i pravila struke.

(7) Svi radnici dužni su u poslovnoj komunikaciji koristiti se službenom elektroničkom adresom (@mioc.hr ili @skole.hr) te ne smiju vlastite elektroničke identitete i pripadajuće lozinke ili pinove davati učenicima i drugim osobama. To se odnosi na personalizirani pristup računalu, matici podataka Grada Zagreba, e-Matici Ministarstva znanosti i obrazovanja, e-Dnevniku, bazi Nacionalnog centra za vanjsko vrednovanje obrazovanja, bazi za upise u srednje škole, ettaedu.hr sustavu, računovodstvenim programima, knjižničarskim programima i ostalim programima ili mrežnim aplikacijama koje sadrže osobne podatke radnika i/ili učenika. Za pristup bežičnoj mreži korisnici škole ovisno o mreži upotrebljavaju AAI@EduHr (skole.hr) ili Active Directory identitet (mioc.hr)

(8) Ako je nužno proslijediti tuđu elektroničku poruku, potrebno ju je proslijediti, a da se pritom ne mijenja kontekst i značenje te paziti da se tuđi osobni podaci ne prosljeđuju bez pristanka vlasnika.

(9) Radnici i vanjski suradnici koji zbog prirode posla imaju pristup osobnim podacima ostalih osoba dužni su pridržavati se svih važećih propisa i etičkih načela iz područja zaštite osobnih podataka te na zahtjev škole o tome potpisati izjavu o tajnosti podataka.

ŠKOLSKA IKT OPREMA I ODRŽAVANJE

Školske računalne mreže

V.

(1) Škola ima računalne mreže:

MREŽA	KONTAKT OSOBA	PRAVO PRISTUPA MREŽI
lokalna mreža s domenom mioc.hr: • računalne učionice • nastavnička i uredska računala • bežična lokalna mreža mioc	voditelj informatičkih učionica ili osoba koju odredi ravnatelj	radnici i ovlašteni vanjski suradnici škole
bežična e-Skole mreža	e-tehničar ili osoba koju odredi ravnatelj	nastavnici i učenici za vrijeme upotrebe interaktivne učionice dobivene u sklopu projekta e-Škole
bežična eduroam mreža	e-tehničar ili osoba koju odredi ravnatelj	radnici i učenici škole uz upotrebu elektroničkog

		identiteta iz sustava AAI@EduHr
--	--	------------------------------------

- (2) Škola može po potrebi definirati privremenu bežičnu mrežu koju definira e-tehničar škole, a pravo pristupa mogu dobiti gosti škole.
- (3) Škola za održavanje računalne infrastrukture u svojoj odgovornosti može zadužiti radnika škole ili angažirati vanjskog suradnika (dalje: sistem inženjer) koji je obavezan u području mioc.hr domene sve potrebne pristupne podatke te svaku promjenu vezanu za održavanje mreže ažurno u osiguranoj omotnici (potpis i pečat škole) pohranjivati u sef škole.
- (4) Ciljevi mjera informacijske sigurnosti koje se primjenjuju na školske računalne mreže jesu omogućavanje elektroničke komunikacije, neometano korištenje informacijama koje su dostupne na računalnoj mreži i zaštita školskih računalnih mreža i zaštita osjetljivih podataka škole.
- (5) Bežične mreže potrebno je prilagoditi tako da samo radnici, učenici i ovlaštene vanjski suradnici (dalje: legitimni korisnici) mogu pristupiti i koristiti se mrežom, a nitko od legitimnih korisnika ne smije ometati i onemogućavati rad školskih bežičnih mreža. Primjerena zaštita pojedine bežične mreže podrazumijeva uključivanje WPA2 standarda na bežičnim pristupnim točkama (engl. *wireless access points*).
- (6) Ako je potrebno spajati se na školska računala s interneta, to je potrebno omogućiti isključivo sigurnosnim protokolom. Preporučeni servisi koji koriste sigurne protokole i koji se preporučuju za spajanje na školska računala s interneta jesu SSH v.2 servis, mrežno sučelje koje omogućuje prijavu korisnika, a koristi se isključivo HTTPS protokol ili VPN.
- (7) Škola, CARNet i Nacionalni CERT zadržavaju pravo nadzora mrežnog prometa.
- (8) Škola treba omogućiti Nacionalnom CERT-u redovite analize ranjivosti računalne mreže te na temelju izvješća poduzeti odgovarajuće aktivnosti.
- (9) Ako CARNet Abuse služba prijavi mrežni incident, škola je dužna u najkraćem mogućem roku otkriti okolnosti u kojima je incident nastao te izvijestiti o svojim aktivnostima CARNet Abuse službu.

Aktivni računalni uređaji u mreži

VI.

- (1) Svi aktivni računalni uređaji u mreži koji su vlasništvo škole (dalje: uređaji) imaju minimalni skup preporučenih sigurnosnih postavki koji uključuje instaliran antivirusni alat, uključen vatrozid, koji onemogućava pristup uređajima s interneta, uključeno automatsko ažuriranje korištenih programa i operacijskog sustava, uz uklanjanje svih računalnih programa koji se ne koriste.
- (2) Uređaji škole konfigurirana su tako da su dio mioc.hr *Active Directory* domene.

(3) 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 sistem inženjera, osobno snosi posljedice, a sistem inženjer ili druga odgovorna osoba nisu dužni popraviti štete koje su nastale upotrebom neovlašteno instaliranog softvera.

(4) Da bi se sve pogodnosti sigurne upotrebe računala primijenila i na prijenosna računala, potrebno ih je redovito najmanje jednom mjesečno uključivati u školsku fiksnu mrežu škole, restartati i omogućiti ažuriranje programa.

(5) Za sva računala i programe koji su dodijeljeni nastavnicima u sklopu projekta e-Škole odgovorne su isključivo te 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 pripadajućim licencama.

(6) Za tablet računala u sklopu interaktivne učionice odgovorni su nastavnici koji održavaju nastavu u tim učionicama.

(7) Na korisnike privatnih uređaja prilikom spajanja na školsku mrežu primjenjuju se sva pravila kao i za ostale školske uređaje i korisnike.

PRIHVATLJIVO I ODGOVORNO KORIŠTENJE INFORMACIJSKO-KOMUNIKACIJSKIM TEHNOLOGIJAMA

Pristup IKT opremi i sigurnost korisnika

VII.

(1) Računala škole koja su u sustavu mioc domene moraju biti prilagođena tako da prije početka rada traže prijavu korisnika sa školskim računom (engl. *account*) u pravilu oblika inicijal imena i prezime (npr. Marko Perić --> mperic)

(2) Računala koja se spajaju na bežične mreže eduroam i e-skole moraju biti prilagođena tako da prije početka rada traže prijavu korisnika autentikacijom na AAI@EduHr sustav.

(3) Preporučuje se korištenje lozinkama koje se sastoje od kombinacije malih i velikih slova, brojki i posebnih znakova i sastoje se od najmanje 8 znakova.

(4) Svi korisnici školskih računala moraju se prijaviti u sustav prije upotrebe i odjaviti nakon završetka korištenja, a to uključuje najmanje upotrebu korisničkog imena i pripadajuće lozinke. Pri pristupu nekim aplikacijama potrebna je upotreba certifikata, odnosno pametne kartice, koji jednoznačno i vjerodostojno identificiraju korisnika, ili kombinacije pina i jednokratne lozinke (*token*)

(5) Korisnici su obvezni čuvati podatke i kartice kojima se koriste za pristup računalima i programima koje će zadržati u tajnosti.

(6) Korisnici se ne smiju koristiti tuđim pristupnim podacima za upotrebu računala. Ako je to potrebno zbog obavljanja radnih zadaća, nužno je zatražiti pisanu suglasnost osobe čiji se

pristupni podaci koriste te suglasnost ravnatelja. Osoba koja je dala svoje pristupne podatke na korištenje mora što prije promijeniti svoje pristupne podatke.

(7) Škola mora osigurati identifikaciju korisnika pojedinog računala u školi jednu godinu nakon upotrebe računala, odnosno iznimno kraće ako su tehničke mogućnosti računalnog sustava u školi ograničavajuće.

(8) Prava pristupa radnika i učenika školskim računalima potrebno je redovito provjeravati i po potrebi mijenjati, a najmanje jedanput godišnje.

(9) Najmanje jedanput godišnje, početkom školske godine, potrebno je revidirati AAI@EDuHr elektroničke identitete učenika.

(10) Učeniku je potrebno ukinuti prava pristupa školskim računalima i isključiti školske elektroničke identitete najkasnije do 31. listopada u godini u kojoj je maturirao, odnosno na dan ispisa iz škole za učenike koji se ispisuju iz škole.

(11) Radniku je potrebno ukinuti prava pristupa školskim računalima i isključiti sve školske elektroničke identitete na dan prestanka radnog odnosa. Iznimno, prema odluci ravnatelja, moguće je produljiti valjanost školskih elektroničkih identiteta radniku i nakon prestanka radnog odnosa radi dovršavanja već započetih poslova.

(12) Datoteke preuzete iz nekog vanjskog izvora (privatna elektronička pošta, vanjska memorija ili internet) mogu ugroziti sigurnost učenika i radnika te se stoga preporuča ne otvarati ili prosljeđivati zaražene datoteke i programe kao ni otvarati datoteke iz sumnjivih ili nepoznatih izvora. U slučaju otvaranja, sve takve datoteke potrebno je provjeriti antivirusnim alatom prije korištenja.

(13) Učenici se smiju koristiti samo školskim računalima koji su namijenjeni za njih u pravilu isključivo za potrebe odgojno-obrazovnog rada, pri čemu moraju paziti da ne ugrožavaju druge korisnike školske mreže širenjem zlonamjernih programa.

(14) Učenici borave u informatičkoj učionici u prisutnosti nastavnika te pristupaju školskim računalima s korisničkim računom koji odredi nastavnik. Nastavnik koji se koristi računalnom učionicom dužan je za svaki nastavni sat imati točan popis rasporeda sjedenja pojedine razredne grupe. Popis je dio nastavničke dokumentacije.

(15) U informatičkoj učionici i pri upotrebi računala u knjižnici nije dopušteno konzumiranje jela i pića.

(16) Učenici su dužni svaki uočeni kvar (hardverski ili softverski) prijaviti nastavniku te ne smiju samovoljno popravljati računala. Učenici na računala ne smiju instalirati nikakve korisničke programe, a ako žele instalirati neki korisnički program, prijedlog mogu uputiti nastavniku informatike ili suradniku u nastavi informatike, koji će uz suglasnost stručnog vijeća nastavnika informatike instalirati predloženi program ako procijeni da je to opravdano.

(17) Na školskom poslužitelju osiguran je diskovni prostor u dvije mape: *upload* i *download*. Za korištenje mapama potrebno je dobiti dodatno odobrenje sistem inženjera. Učenici se mogu služiti mapom *download* kako bi iz te mape preuzeli određenu datoteku ili mapu, a mapu *upload* kako bi u nju postavili svoju datoteku ili mapu. U mapu *download* nije moguće bez dodatnog

odobrenja postaviti neku datoteku, dok iz mape *upload* nije moguće bez dodatnog odobrenja preuzeti datoteku.

(18) Škola može odrediti svoj diskovni prostor u oblaku. Politika ponašanja na diskovnom prostoru u oblaku određuje se prema uputama odgovorne osobe.

(19) Učenici smiju koristiti multimedijske sadržaje, programe za suradnju i komunikaciju, društvene mreža te slične načine komunikacije tijekom nastave samo uz dopuštenje nastavnika. Određeni neprimjereni internetski sadržaji nisu dostupni učenicima na školskoj mreži. Škola može zatražiti od CARNeta, odnosno MZO-a reviziju filtriranog sadržaja. Učenici su dužni prihvatiti filtriranje određenih sadržaja kao sigurnosnu mjeru te ga ne smiju pokušati zaobići. 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 nastavnika.

(20) Učenici se smiju koristiti školskim računalima u privatne svrhe, koja su određena za to, isključivo u slobodno vrijeme (za vrijeme odmora i prije ili poslije nastave).

(21) Tijekom odgojno-obrazovnog rada učenici se iznimno smiju koristiti vlastitim uređajima samo za potrebe nastave uz prethodno dopuštenje predmetnog nastavnika.

Ponašanje na internetu

VIII.

(1) Korisnici su dužni prilikom upotrebe IKT opreme primjenjivati osnovna pravila lijepog ponašanja, ponašati se odgovorno i u skladu s etičkim načelima i u stvarnom i u virtualnom svijetu. Prema drugim korisnicima moraju se ponašati pristojno, ne smiju ih vrijeđati ili objavljivati neprimjerene sadržaje.

(2) Svi korisnici, a posebno učenici, moraju znati da su odgovorni za sve što pišu, objavljuju ili komentiraju na internetu te trebaju biti svjesni publike (kolege, potencijalni poslodavci, suradnici i sl.). Uvijek moraju imati na umu da i njihova privatna aktivnost u društvenim medijima može utjecati na školske rezultate te da su njihove aktivnosti dostupne za pregled drugim korisnicima.

(3) Fotografiranje i snimanje osoba smije se napraviti samo uz prethodnu dopuštenje. Potrebno je imati dopuštenje za objavu takvih digitalnih sadržaja.

(4) Korisnici su odgovorni za sve neželjene posljedice upotrebe interneta. Da bi se izbjegle neugodne i neželjene situacije, škola predlaže korisnicima da dobro razmisle o sadržaju koji objavljuju.

(5) Korisnici moraju promišljeno dijeliti svoje osobne podatke na internetu te osvijestiti da, kad se jednom podatak pojavi na internetu, više ga nije moguće trajno ukloniti. Prilikom dijeljenja tuđih osobnih podataka korisnici su dužni pridržavati se važećih propisa iz područja zaštite osobnih podataka i tajnosti podataka.

(6) Korisnici se prilikom dijeljenja privatnih i školskih informacija trebaju voditi načelima otvorenosti i transparentnosti te zaštite privatnosti. U svrhu zaštite privatnosti učenika i radnika,

škola preporučuje radnicima upotrebu zatvorenih privatnih profila na društvenim mrežama, a da pritom ne prihvataju učenika kao prijatelja.

(7) Učenici trebaju dobro uravnotežiti vrijeme za korištenje internetom s drugim oblicima nastave, učenja i odmora.

(8) Učenici i radnici educirat će se o odgovornoj upotrebi interneta u okviru aktivnosti predviđenih školskim kurikulumom, odnosno pohađat će edukacije u sklopu stručnog usavršavanja.

Autorsko pravo i intelektualno vlasništvo

IX.

(1) U svrhu poštivanja propisa o zaštiti autorskog prava i intelektualnog vlasništva, korisnike se potiče da potpisuju materijale koje su sami izradili te da ih označuju sa željenim licencama, poštuju tuđe radove, a to znači da je zabranjeno tuđe radove predstavljati kao svoje, preuzimati zasluge za tuđe radove ili ih nedopušteno preuzimati s interneta. Pri upotrebi tuđih materijala s interneta mora se citirati i navesti autora korištenih materijala te izvor informacije (poveznica i datum preuzimanja). Svaki korisnik odgovoran je za poštivanje autorskih prava i intelektualnog vlasništva.

(2) Za fotografiranje i snimanje tuđih radova (prezentacija, plakata, tiskanih materijala) potrebno je imati dozvolu autora rada.

(3) Korisnici moraju imati na umu da sadržaji koji se nalaze na internetu ne moraju biti provjereni ni istiniti, stoga je sve podatke s interneta potrebno kvalitetno vrednovati. Učenici se svakako trebaju koristiti informacijama s interneta u skladu s nastavničkim uputama. Svi sadržaji koji se koriste kao izvor informacija za nastavu moraju se koristiti iz provjerenih izvora.

(4) Pri dijeljenju datoteka na internetu treba biti posebno oprezan, tj. treba poštivati ne samo autorska prava već i uvjete dijeljenja sadržaja ako je to dopušteno. Primjer nelegalnog dijeljenja datoteke jest umnožavanje ili preuzimanje autorski zaštićenog materijala poput *online* knjige, glazbe ili pak video sadržaja. Upotreba programa koji omogućuju dijeljenje sadržaja između računala (kao što je *torrent*) najčešće omogućuju nelegalno dijeljenje video i glazbenih sadržaja, ključeva za upotrebu različitih aplikacija i drugih digitalnih sadržaja. Izričito je zabranjeno daljnje distribuiranje i umnožavanje takvih sadržaja bez dopuštenja autora ili bez plaćanja naknade jer su zaštićeni autorskim pravima..

Internetsko nasilje

X.

(1) Zabranjen je svaki oblik internetskog nasilja, kao na primjer, nastavljanja slanja e-pošte usprkos tome što netko više ne želi komunicirati ili kontaktirati s pošiljateljem, otkrivanje osobnih podataka žrtve na mrežnim stranicama ili forumima, lažno predstavljanje žrtve na internetu, slanje prijetećih poruka žrtvi koristeći različite internetske servise za komunikaciju, postavljanje internetske ankete o žrtvi, slanje zlonamjernih programa na e-adresu ili mobitel i slanje uznemirujućih slika različitim komunikacijskim alatima.

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

(3) U slučaju saznanja za događaje internetskog nasilja počinjenih prema učenicima, škola je dužna poduzeti potrebne korake i obavijestiti nadležne institucije u skladu s posebnim propisima.

PRIJELAZNE I ZAVRŠNE ODREDBE

XI.

(1) Ova Odluka stupa na snagu osmog dana od dana objave na oglasnoj ploči.

(2) Danom stupanja na snagu ove Oduke prestaje vrijediti Odluka o prihvatljivom korištenju računalnih resursa XV. gimnazije u Zagrebu, KLASA: 003-06/13-01, URBROJ: 251-94/23-35 od 30. rujna 2013. godine.

KLASA: 003-05/17-01/05

URBROJ: 251-94-08-17-1

Zagreb, 12. prosinca 2017.

PREDSJEDNICA
ŠKOLSKOG ODBORA
Marina Bilić, dipl. ing.

Ova Odluka donesena je dana 11. prosinca 2017. godine, objavljena je na oglasnoj ploči dana 13. prosinca 2017. godine, a stupa na snagu dana 21. prosinca 2017. godine.

RAVNATELJICA
Ljiljana Crnković, prof.