XV. GIMNAZIJA

ZAGREB, Jordanovac 8

ODLUKA
O PRIHVATLJIVOM KORIŠTENJU
RAČUNALNIH RESURSA
XV. GIMNAZIJE U ZAGREBU

Zagreb, 2013.

Na temelju članka 26. Statuta XV. gimnazije (pročišćeni tekst od 5. travnja 2013. godine Školski odbor na sjednici održanoj 30. rujna 2013. godine donosi

ODLUKU
O PRIHVATLJIVOM KORIŠTENJU RAČUNALNIH RESURSA
XV. GIMNAZIJE U ZAGREBU

Uvod

Svrha Odluke o prihvatljivom korištenju računalnih mreža u XV. gimnaziji, Zagreb (u daljnjem tekstu Škole) je jasno određivanje načina dopuštenog i prihvatljivog korištenja mreža Škole i njihovih usluga.

Odluka vrijedi za sve korisnike računalne infrastrukture Škole. Obveza je Škole osigurati da se na području njezine odgovornosti korisnici ponašaju u skladu s odredbama Odluke o prihvatljivom korištenju CARNet mreže.

Sigurnosna politika

Ljudski i informacijski resursi se smatraju najvažnijim vrijednostima Škole. Stoga je za sigurno rukovanje informacijama potrebno uspostaviti pravila njihova korištenja kao i ponašanja njihovih korisnika. U tom smislu je prihvatljivo korištenje mrežnih i računalnih resursa Škole od iznimne važnosti.

S obzirom da rad Škole ovisi i o radu školske infrastrukture, školska računala (i druga školska računalna imovina) moraju biti podešena tako da omoguće neometan pristup i korištenje informacija potrebnih u nastavi i drugim aktivnostima vezanim za rad Škole.

Cilj ove Odluke je povećanje sigurnosti rada i učenja u školi.

Odluka o prihvatljivom korištenju računalnih resursa odnose se na sve aspekte sigurnosti, a primjenjuju se na cjelokupnu Školsku računalnu infrastrukturu (sva računala: stolna i prijenosna, mrežne uređaje, ulazno izlazne uređaje te mobilne uređaje). Pravila se odnose na sve osobe koje koriste školsku infrastrukturu.

Djelatnici škole i učenici su korisnici školske informatičke opreme i mreže. Korisnici ne smiju uništavati školsku informatičku opremu.

Svako nepridržavanje ovih pravila ima negativan utjecaj po Školu i može rezultirati disciplinskim mjerama prema djelatnicima Škole ili pedagoškim mjerama prema učenicima. Svako ponašanje protivno ovoj Odluci potrebno je prijaviti odgovornoj osobi (nastavnik ili

administrator resursa ili sistem inženjer mreže ili voditelj informatičkih učionica) ili ravnatelju škole. Za nepridržavanje ovih pravila posljedice snosi pojedinac.

Sigurnost informacija

Načelo povjerljivosti informacija podrazumijeva da informacije moraju biti dostupne samo onome kome su namijenjene. U skladu s ovim načelom Škola razlikuje javne i interne informacije.

Skupinu javnih informacija čine one informacije koje opisuju djelatnosti Škole, a njihova javna dostupnost je u interesu Škole. Tu spadaju kontaktni podaci Škole, promidžbeni materijali, internetske stranice Škole, Katalog informacija i sl.

Interne informacije su one informacije koje se odnose na osobne podatke pojedinaca (npr. kontakt podaci osobe, fotografije osobe, podaci iz evidencija koje vodi Škola (Razredna knjiga, Imenik učenika, registri, matične knjige, e-dnevnik, e-matice) te informacije koje su namijenjene samo djelatnicima Škole. Tuđe osobne podatke zabranjeno je koristiti bez dopuštenja osobe odgovorne za te podatke.

Poslovnu dokumentaciju važnu za poslovanje Škole, održavanje nastave te druge važne dokumente je potrebno čuvati na zakonom propisani način. Vremenski rokovi su zadani Zakonom o računovodstvu i popisom Hrvatskog državnog arhiva te ostalim propisima koji uređuju vremena čuvanja i pohrane poslovne i školske dokumentacije.

Sigurnosna preslika je kopija podatak na drugom mediju za pohranu podataka. Kako bi se spriječilo nepovratno oštećenje ili gubitak podataka, za sve podatke koje se pohranjuju na računalima Škole, a za koje Škola procijeni da su važne potrebno je redovito izrađivati njihovu sigurnosnu presliku.

Mjere fizičke sigurnosti primjenjuju se na sva mjesta gdje se nalaze podaci važni za rad Škole. Te mjere moraju biti dogovorene i usklađene s pozitivnom zakonima o sigurnosti podataka.

Svi nastavnici i zaposlenici Škole dužni su u svojoj poslovnoj komunikaciji koristiti službenu elektroničku adresu (@mioc.hr).

Nastavnici i zaposlenici škole ne smiju vlastite elektroničke identitete i pripadne lozinke ili pinove davati učenicima. To se odnosi na personalizirani pristup: računalu, matici podataka Grada Zagreba, MZOS matici, e-dnevniku, bazi NCVVO-a, bazi za upise u srednje škole, ettaedu.eu sustavu, računovodstvenim programima, knjižničarskim programima i ostalim programima ili web aplikacijama koje sadrže osobne podatke zaposlenika i/ili učenika.

Nastavnici, zaposlenici Škole te vanjski suradnici koji radi prirode posla imaju pristup osobnim podacima ostalih osoba dužni se pridržavati svih pozitivnih zakona i etičkih načela te o tome potpisati izjavu o „tajnosti podataka“.

Struktura školskih računalnih mreža i definiranje odgovornost o održavanju:

Škola ima tri osnovne računalne mreže:

1. Lokana mreža s domenom mioc.hr (u nadležnosti Škole):
    a. računalne učionice
    b. nastavnička i uredska računala
    c. WiFi lokalna mreža mioc (područje učionica za nastavu informatike)
2. WiFi e-dnevnik mreža (u nadležnosti CARNet-a),
3. WiFi eduroam mreža (u nadležnosti CARNet-a).

Definiranje odgovornosti o održavanju računalnih mreža:

1. Lokana mreža s domenom mioc.hr : odgovorna Škola
2. WiFi e-dnevnik mreža (CARNet): odgovoran CARNet, kontakt osoba za Školu voditelj informatičkih učionica ili osoba koju odredi Ravnatelj
3. WiFi eduroam mreža (CARNet): odgovoran CARNet, kontakt osoba za Školu voditelj informatičkih učionica ili osoba koju odredi Ravnatelj

Škola za održavanje računalne infrastrukture u svojoj odgovornosti može zadužiti djelatnika škole ili angažirati vanjskog suradnika (u daljnjem tekstu Sistem inženjer). Sistem inženjer u području mioc.hr domene obvezuje se da sve potrebne pristupne podatke vezane za održavanje mreže ažurno, u osiguranoj omotnici (potpis i pečat Škole) pohranjuje u sefu Škole.

Sigurnost školske računalne mreže

Ciljevi mjera informacijske sigurnosti koje se primjenjuju na školsku računalnu mrežu su, kako slijedi:

1. omogućavanje elektroničke komunikacije,
2. neometano korištenje informacija koje su putem računalne mreže dostupne,
3. zaštita školskih računalnih mreža,
4. zaštita osjetljivih podataka Škole.

Potrebno je dokumentirati izgled mreže. Dokumentacija može obuhvaćati grafički prikaz fizičkog rasporeda računala u Školi uključujući osnovne postavke (IP adresa računala), ili popis računala s informacijom gdje su smještena te koje IP adrese imaju dodijeljene.

Bežične mreže (WiFi) je potrebno je podesiti tako da samo legitimni korisnici mogu pristupiti i koristiti mrežu. Legitimni korisnici mogu biti nastavno i administrativno tehničko osoblje te učenici. Nitko od navedenih korisnika ne smije ometati i onemogućavati rad školskih bežičnih

mreža. Primjerena zaštita pojedine bežične mreže podrazumijeva uključivanje WPA/WPA2 standarda na bežičnim pristupnim točkama (eng. wireless access points).

Pravo pristupa WiFi mrežama unutar škole imaju:

1. WiFi lokalna mreža mioc: nastavnici informatike
2. WiFi e-dnevnik mreža (CARNet): isključivo nastavnici uključeni u korištenje aplikacije e-dnevnik
3. WiFi eduroam mreža (CARNet): učenici i radnici Škole korištenjem aai identiteta

Nisu svi sadržaji na Internetu primjereni za učenike ili nastavu. Iz tog razloga određeni sadržaji nisu dostupni učenicima kroz školsku mrežu (filtrirani su). Škola može zatražiti od CARNeta, odnosno MZOS-a reviziju filtriranog sadržaja.

Škola, CARNet i CERT zadržavaju pravo nadzora mrežnog prometa.

Ukoliko je potrebno spajati se na školska računala s Interneta, to je potrebno omogućiti isključivo putem sigurnih protokola. Neki servisi koji koriste sigurne protokole i koje se preporuča koristiti za spajanje na školska računala s Interneta su SSH v.2 servis, web sučelje koje omogućuje prijavu korisnika a koristi isključivo HTTPS protokol ili VPN.

Sigurnost školskih računala:

Ispravna konfiguracija računala olakšava njihovo održavanje, a ujedno i povećava sigurnost učenika i nastavnika odnosno ostalih zaposlenika škole. Zato je potrebno da sva računala u školi imaju minimalni skup preporučenih sigurnosnih postavki. Sva računala trebaju imati instaliran antivirusni alat. Sva računala moraju imati uključen vatrozid (engl. firewall) kako bi se onemogućio pristup do njih s Interneta. Potrebno je redovito ažurirati sve programe na računalima. Zato je potrebno uključiti automatsko ažuriranje (engl. update) korištenih programa i korištenog operacijskog sustava. Preporučuje se sve računalne programe koji se ne koriste ukloniti s računala.

Sva računala škole konfigurirana su tako da su dio mioc domene. Na taj način su za sva računala osigurane sve sigurnosne mjere u smislu antivirusnih provjera, ažuriranja programa te je onemogućeno i zabranjeno samovoljno instaliranje softvera. Svi programi instalirani i korišteni na računalima moraju imati licenciju ili moraju biti u kategoriji slobodnog softvera ili u kategoriji probnih inačica softvera.

Ukoliko netko koristi nelegalan softver ili softver koji je instalirao bez dozvole Sistem inženjera za sve štete osobno snosi krivicu. Sistem inženjer ili druga odgovorna osoba nisu dužni sanirati štete nastale korištenjem neovlašteno instaliranog softvera.

Kako bi se sve pogodnosti sigurnog korištenja računala primijenila i na prijenosna računala potrebno ih je redovito (minimalno jednom mjesečno) uključivati u školsku mrežu (spojiti mrežnim kabelom) i omogućiti ažuriranje programa.

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

Računala koja se spajaju na WiFi mreže eduroam i e-dnevnik moraju biti podešena tako da prije početka rada traže prijavu korisnika autentikacijom putem AAI sustava.

Preporučuje se korištenje lozinki koje se sastoje od kombinacije malih i velikih slova, brojeva i posebnih znakova te su minimalne duljine 10 znakova.

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

Učenici na računala ne smiju instalirati nikakve korisničke programe. Ako učenici žele instalirati neke korisničke programe, mogu se obratiti svom nastavniku informatike, suradniku u nastavi informatike ili ravnatelju škole.

Sigurnost korisnika

Podizanje razine svijesti korisnika o važnosti sigurnosti ključno je za uspješno provođenje ovih pravila. Korisnici moraju biti dobro upoznati sa sigurnosnim aspektima pri korištenju računala i mjerama koje proizlaze iz njega, a to se postiže redovitom edukacijom. Potrebno je što više napora uložiti u edukaciju učenika i nastavnika te ostalih zaposlenika o sigurnosnim aspektima prilikom korištenja računala i mobilnih uređaja.

Svi korisnici školskih računala moraju se prijaviti na sustav prije korištenja i odjaviti nakon završetka korištenja. Prijava i odjava korisnika mora uključivati minimalno korištenje korisničkog imena i pripadajuće lozinke. Kod pristupa nekim aplikacijama potrebno je korištenje certifikata odnosno pametne kartice koji jednoznačno i vjerodostojno identificiraju korisnika ili kombinacije pina i jednokratne lozinke (token).

Korisnici su obvezni čuvati podatke i kartice koje koriste za pristup računalima i programima tajnima. Korisnici ne smiju koristiti tuđe pristupne podatke za korištenje računala. Ako je to potrebno zbog obavljanja radnih zadaća, nužno je tražiti suglasnost osobe čiji pristupni podaci se koriste te suglasnost ravnatelja. Osoba koja je (iz objektivnih razloga) dala svoje pristupne podatke na korištenje mora što prije promijeniti svoje pristupne podatke.

Škola mora osigurati identifikaciju korisnika pojedinog računala u Školi godinu dana nakon korištenja računala, odnosno iznimno kraće ukoliko su tehničke mogućnosti računalnog sustava u Školi ograničavajuće.

Ako je nužno proslijediti tuđu elektroničku poruku (eng. e-mail), poruku je potrebno proslijediti bez mijenjanja konteksta i značenja. Prilikom prosljeđivanja tuđe elektroničke poruke potrebno je paziti da se tuđi osobni podaci ne prosljeđuju bez pristanka vlasnika.

Datoteke preuzete iz nekog vanjskog izvora (putem elektroničke pošte, vanjske memorije, ili s Interneta) mogu ugroziti sigurnost učenika, nastavnika i ostalih zaposlenika škole. 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.

Prava pristupa učenika i zaposlenika škole školskim računalima potrebno je redovito provjeravati i po potrebi mijenjati, minimalno jednom godišnje.

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

Zadnji nastavni dan učenika odnosno radni dan nastavnika u Školi potrebno je isključiti sva njegova prava pristupa školskim računalima. Nakon isteka učeničkog statusa i prestanka potrebe za posjedovanjem elektroničkog identiteta učenika, identitet je potrebno isključiti.

Učeniku je potrebno ukinuti prava pristupa školskim računalima i isključiti školske elektroničke identitete najkasnije 1. listopada u godini u kojoj je završio četvrti razred, odnosno danom ispisa iz škole za učenike koji se ispisuju iz škole prije završenog četvrtog razreda.

Zaposleniku Škole potrebno je ukinuti prava pristupa školskim računalima i isključiti sve školske elektroničke identitete danom isteka ugovora o radu u Školi. Iznimno, uz odluku Ravnatelja, moguće je produljiti valjanost školskih elektroničkih identiteta zaposleniku i nakon prestanka radnog odnosa u Školi, a radi dovršavanja već započetih poslova.

Učenici smiju koristiti samo školska računala namijenjena njima. Vlastita računala i pametne telefone tijekom nastave učenici smiju koristiti isključivo u obrazovne svrhe uz prethodnu dozvolu nastavnika. Pri tome učenici moraju paziti da ne ugrožavaju druge korisnike Školske mreže širenjem virusa i drugih zlonamjernih programa.

Učenici smiju koristiti školska računala u privatne svrhe isključivo u slobodno vrijeme (za vrijeme odmora, te prije ili nakon nastave). Učenici ne smiju ometati druge učenike ili nastavnike prilikom korištenja računala tijekom boravka u Školi ili oko Škole.

Učenici pristupaju školskim računalima unutar informatičkih učionica s korisničkim računom koji odredi nastavnik. Nastavnik koji koristi računalnu učionicu dužan je za svaki nastavni sat imati točan raspored sjedenja pojedine razredne grupe. Popis je dio nastavničke dokumentacije.

Učenici borave u informatičkoj učionici u prisutnosti nastavnika. U informatičkoj učionici nije dozvoljeno konzumiranje jela i pića. Ukoliko učenik primijeti neki kvar (hardverski ili softverski) o tome treba odmah obavijestiti nastavnika. Učenicima nije dozvoljeno samovoljno „popravljanje“ računala.

Na školskom serveru osiguran je diskovni prostor kojem mogu pristupiti učenici i nastavnici. Radi sigurnosti i dobroga korištenja mrežnih resursa definirane su dvije mape (upload i download). Nastavnici mogu pristupati i koristiti obje mape. Za korištenje mapa potrebno je dobiti dodatno odobrenje od odgovorne osobe (Sistem inženjer). Nastavnici (koji nemaju dodatno odobrenje) i učenici mogu koristiti mapu „download“ kako bi iz te mape preuzeli

određenu datoteku ili mapu, a mapu „upload“ kako bi u tu mapu postavili svoju datoteku ili mapu. U mapu „download“ nije moguće bez dodatnog odobrenja postaviti neku mapu ili datoteku, a iz mape „upload“ nije moguće (bez dodatnog odobrenja) preuzeti datoteku ili mapu.

Politika prihvatljivog korištenja informacijsko komunikacijskih tehnologija

Učenike i nastavnike se potiče na korištenje informacijskih tehnologija i alata u svrhu unapređenja obrazovanja. Korištenje multimedijskih sadržaja, programa za suradnju i komunikaciju, društvenih mreža te sličnih načina komunikacije tijekom nastave je dozvoljeno samo ako to nastavnik dopusti.

Korisnici školskih računala se moraju ponašati odgovorno i u skladu s etičkim načelima i u stvarnom i u virtualnom svijetu. Prema drugim korisnicima moraju se ponašati pristojno, ne vrijeđati ih niti objavljivati neprimjerene sadržaje.

Prilikom korištenja i objavljivanja sadržaja na Internetu, uputno je da se korisnici pridržavaju sljedećih naputaka:

- *odgovornost za sadržaje* - svi korisnici, a posebice učenici, moraju znati da su odgovorni za sve što pišu, objavljuju ili komentiraju na Internetu. Uvijek moraju imati na umu da i njihova privatna aktivnost u društvenim medijima može utjecati na školske rezultate. Učenici mogu gledati sve nastavničke aktivnosti na Internetu, ali i obrnuto. Svaki korisnik je odgovoran i za sve neželjene posljedice korištenja Interneta. Kako bi se izbjegle neugodne/neželjene situacije predlažemo korisnicima da u svakoj situaciji, gdje god bili i o kojoj god temi objavljivali sadržaje, dobro razmisle o sadržaju koji objavljuju.

- *potpisivanje* - odgovorni korisnici svojim potpisom stoje iza sadržaja koje objave na Internetu. Korisnike se potiče da se, gdje god smatraju primjerenim, predstave svojim imenom. Time nastaje bolja društvena mreža kontakata, a i drugi korisnici će radije koristiti sadržaje iz poznatih izvora.

- *znanje o publici* - 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 itd.

- *razumijevanje koncepta zajednice* - društvene mreže (zajednice) postoje kako bi se njihovi članovi mogli međusobno podržavati. Zato svaki korisnik mora dobro balansirati između privatnih i školskih informacija koje dijeli s drugima. Vrlo važnu ulogu u razvoju i osnaživanju zajednice imaju otvorenost i transparentnost. Takva zajednica ne potiče suparništvo, već suradnju i međusobno pomaganje.

- *poštivanje autorskih prava* - 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).

- *čuvanje vlastite i tuđe privatnosti* - korisnici moraju biti pažljivi koje svoje osobne podatke objavljuju na Internetu jer time utječu na svoju sigurnost i zaštitu svoje privatnosti. Nadalje, korisnici moraju biti svjesni činjenice da kad se jednom podatak pojavi na Internetu više ga nije moguće jednostavno ukloniti.
- *umjerenost u korištenju* - vrlo je bitno dobro uravnotežiti vrijeme odvojeno za korištenje Interneta, s drugim oblicima nastave, učenja i odmora.

Korisnici moraju imati na umu da sadržaji koji se nalaze na Internetu ne moraju biti provjereni niti istiniti. Zato sve činjenice koje nađu na Internetu moraju koristiti s oprezom. Učenici svakako trebaju koristiti informacije s Interneta u skladu s nastavnikovim uputama. Svi sadržaji koji se koriste kao izvor informacija za nastavu moraju se koristiti iz provjerenih izvora.

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 svom nastavniku ili nastavniku informatike. Ako učenici primijete neprimjerene, uznemirujuće ili sadržaje koji ugrožavaju njihovu sigurnost, o tome odmah trebaju obavijestiti svog nastavnika, nastavnika informatike, nastavnika iz stručno razvojne službe škole ili ravnatelja.

Učenici se moraju pridržavati i drugih uputa koje im mogu dati nastavnici, a koje imaju za cilj unaprjeđenje sigurnosti školske informatičke opreme i mreže.

Ova odluka stupa na snagu danom donošenja.

Klasa: 003-06/13-01
Urbroj: 251-94/23-35
Zagreb, 30.09.2013.

PREDSJEDNICA
ŠKOLSKOG ODBORA

Marina Bilić, dipl. ing.