REPUBLIKA HRVATSKA
UPRAVNA ŠKOLA ZAGREB
Prilaz baruna Filipovića 30
10000 Zagreb
Tel/fax: 01 4830 774
E-mail: ured@ss-upravnaskolazagreb-zg.skole.hr

KLASA: 602-03/16-02-01/325
URBROJ: 251-283-16-02-1

U Zagrebu, 23.11.2016.

PRIHVATLJIVO KORIŠTENJE RAČUNALA U UPRAVNOJ ŠKOLI ZAGREB

Ravnateljica:

_____
Suzana Hitrec, prof.

Sadržaj

Uvod

Ljudski i informacijski resursi se smatraju najvažnijim vrijednostima Upravne škole Zagreb (u Škola). Stoga je za sigurno rukovanje informacijama potrebno uspostaviti pravila njihova korištenja kao i ponašanja njihovih korisnika.

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

Cilj ovih pravila je povećanje sigurnosti rada i učenja u Školi. Pravila prihvatljivog korištenja odnose se na sve aspekte sigurnosti, a primjenjuju se na cjelokupnu školsku računalnu infrastrukturu (sva računala, mobilne i mrežne uređaje u Školi). 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 ovim pravilima potrebno je prijaviti nastavniku ili ravnatelju Škole.

1. 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, matične knjige) 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 dokumentacije.

Sigurnosna preslika je kopija informacija na drugom računalu. Kako bi se spriječilo nepovratno oštećenje ili gubitak informacija, za sve informacije koje se pohranjuju na računalima Škole, a za koje Škola procijeni da su važne, redovito se izrađuje njihova sigurnosna preslika.

Mjere fizičke sigurnosti primjenjuju se na sva mjesta gdje se nalaze informacije važne za rad Škole. Te mjere su unaprijed dogovorene i obuhvaćaju zaključavanje ormarića i prostorija gdje se važne informacije pohranjuju.

2. 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 školske računalne mreže,
4. zaštita osjetljivih podataka Škole

Mreža je podijeljena u manje cjeline (podmreže) pri čemu je uzeto u obzir organizacijski i funkcionalni kriterij. Na taj način moguće je odvojiti skupine korisnika, odnosno računala zaposlenika Škole od učeničkih.

Mreža se dijeli na mrežne cjeline:

- Administracija - obuhvaća sva računala kojima se služi dio zaposlenika Škole za potrebe Tajništva škole, računovodstva i drugog općeg poslovanja Škole. Učenici nemaju pristup ovoj mrežnoj cjelini.
- Učionica - obuhvaća sva računala u učionicama. Ovim računalima imaju pristup učenici i nastavnici Škole.

Radi lakšeg održavanja izgled mreže je dokumentiran. Dokumentacija obuhvaća grafički prikaz fizičkog rasporeda računala u Školi uključujući osnovne postavke (IP adresa računala), i popis računala s informacijom gdje su smještena te koje IP adrese imaju dodijeljene.

Bežična mreža (WiFi) podešena je tako da samo legitimni korisnici mogu pristupiti i koristiti mrežu. Legitimni korisnici mogu biti nastavno i administrativno osoblje. Nitko od navedenih korisnika ne smije ometati i onemogućavati rad školske bežične mreže.

Ako je potrebno spajati se na školska računala s Interneta, to se omogućuje 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.

Nisu svi sadržaji na Internetu primjereni za učenike ili nastavu. Iz tog razloga određeni sadržaji nisu dostupni učenicima kroz školsku mrežu (filtrirani su).

Škola zadržava pravo nadzora mrežnog prometa.

3. Sigurnost školskih računala

Ispravna konfiguracija računala olakšava njihovo održavanje, a ujedno i povećava sigurnost učenika i nastavnika. Zato je potrebno da sva računala u Školi imaju minimalni skup preporučenih sigurnosnih postavki. Sva računala imaju instaliran antivirusni alat Microsoft Security Essentials. Sva računala imaju uključen vatrozid (eng. firewall) kako bi se onemogućio pristup do njih s Interneta. Svi programi na računalima su redovito ažurirani.

Računala su podešena tako da traže prijavu korisnika (npr. autentikacijom putem AAI sustava) prije početka rada. Koriste se lozinke koje se sastoje od kombinacije malih i velikih slova, brojeva i posebnih znakova te su minimalne duljine 8 znakova.

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

Učenici na računala ne smiju instalirati nikakve korisničke programe bez dozvole. Ako učenici žele instalirati neke korisničke programe, mogu se obratiti svom nastavniku informatike .

4. Sigurnost korisnika

Podizanje razine svijesti korisnika o važnosti sigurnosti ključno je za uspješno provođenje ovih pravila. Korisnici su dobro upoznati sa sigurnosnim aspektima pri korištenju računala i mjerama koje proizlaze iz njega, a to se postiže redovitom edukacijom.

Svi korisnici školskih računala moraju se prijaviti na sustav prije korištenja i odjaviti nakon završetka korištenja. Prijava i odjava korisnika uključuje korištenje korisničkog imena i pripadajuće lozinke.

Korisnici su obvezni čuvati podatke 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. Osoba koja je dala svoje pristupne podatke na korištenje mora što prije promijeniti svoje pristupne podatke.

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

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, vanjskog diska, ili s Interneta) mogu ugroziti sigurnost učenika ili nastavnika. 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.

Pravila pristupa učenika i zaposlenika Škole školskim računalima redovito se provjeravaju i po potrebi mijenjaju. Minimalno jednom godišnje (početkom školske godine) revidiraju se elektronički identiteti (AAI) učenika. Zadnji nastavni dan učenika odnosno radni dan nastavnika u Školi isključuju se sva njegova prava pristupa školskim računalima. Nakon isteka učeničkog statusa i prestanka potrebe za posjedovanjem elektroničkog identiteta učenika, identitet je neaktivan.

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.

5. Politika prihvatljivog korištenja

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 ponašaju odgovorno i u skladu s etičkim načelima i u stvarnom i u virtualnom svijetu. Prema drugim korisnicima se ponašaju pristojno, ne vrijeđaju ih niti objavljuju neprimjerene sadržaje.

Prilikom korištenja i objavljivanja sadržaja na Internetu, korisnici se 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.

- *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 informatike. Ako učenici primijete neprimjerene, uznemirujuće ili sadržaje koji ugrožavaju njihovu sigurnost, o tome odmah trebaju obavijestiti svog nastavnika informatike.

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