

Smjernice za sigurno ponašanje u radu s računalima

Cilj ovih pravila jest osiguravanje sigurnosti korištenja računala unutar predškolske ustanove (dalje u tekstu: Ustanova). Pravila se odnose na korištenje službenih računala te mobilnih i mrežnih uređaja. Obvezujuća su za sve osobe koje se njima koriste (djelatnici Ustanove i djeca).

Sigurnost informacija

Načelo povjerljivosti informacija podrazumijeva da informacije trebaju biti dostupne samo onome kome su namijenjene:

1. Javne informacije opisuju djelatnosti vrtića i dostupne su na mrežnim stranicama vrtića. Njihova dostupnost je u interesu vrtića. U javne informacije spadaju kontaktni podatci vrtića, podatci o svim objektima, internetska stranica vrtića, katalog informacija i slično.

2. Interne informacije se odnose na osobne podatke pojedinaca (kontakt podaci osobe, podaci iz evidencija koje vodi Ustanova (matična knjiga upisane djece, imenici djece) kao i informacije koje su namijenjene samo djelatnicima Ustanove. Tuđe osobne podatke zabranjeno je koristiti bez dopuštenja osobe odgovorne za te podatke.

Poslovnu dokumentaciju važno za poslovanje Ustanove, provođenje neposrednog pedagoškog rada te ostale važne dokumente, potrebno je čuvati na zakonom propisani način. Vremenski rokovi čuvanja istih, zadani su Zakonom o računovodstvu te propisom Hrvatskog državnog arhiva te ostalim propisom koji uređuju vremena čuvanja i pohrane poslovne dokumentacije.

Sigurnosna preslika jest kopija informacija na drugom računalu. Kako bi se preveniralo nepovratno oštećenje ili gubitak informacija, za sve informacije koje se pohranjuju na računalima Ustanove, a za koje Ustanova procijeni da su važne, potrebno je kontinuirano izrađivati njihovu sigurnosnu presliku.

Mjere fizičke sigurnosti primjenjuju se na sva mjesta gdje se nalaze informacije važne za rad Ustanove. Takve mjere moraju biti unaprijed dogovorene i moraju minimalno obuhvaćati zaključavanje ormarića ili prostorija gdje se važne informacije pohranjuju.

Sigurnost računala u Ustanovi

Ciljevi i mjere informacijske sigurnosti jesu:

1. Omogućavanje elektroničke komunikacije
2. Neometano korištenje informacija koje su putem računala dostupne
3. Zaštita podataka Ustanove
4. Zaštita računala Ustanove

Bežičnu mrežu (WiFi) potrebno je podesiti tako da samo legitimni korisnici mogu pristupiti i koristiti mrežu. Legitimni korisnici mogu biti nastavno i nenastavno osoblje te djeca uz nadzor odgojitelja. Sva računala moraju imati instaliran antivirusni alat. U tu svrhu se koriste besplatni antivirusni alati. Sva računala moraju imati uključen vatrozid („firewall“). Potrebno je redovito ažurirati sve programe na računalima Ustanove. U tu svrhu potrebno je uključiti automatsko ažuriranje („update“) programa

koji se koriste i korištenog operativnog sustava. Preporučuje se uklanjanje s računala Ustanove svih računalnih programa koji se ne koriste.

Računala moraju biti podešena tako da traže prijavu korisnika prije početka rada. Predlaže se korištenje lozinki koje se sastoje od kombinacije malih i velikih slova te brojeva i posebnih znakova ukupne duljine najmanje 8 znakova.

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

Djeca uključena u redovite programe Ustanove pristupaju računalu isključivo pod nadzorom odgojitelja.

Sigurnost korisnika

Podizanje razine svijesti korisnika o važnosti sigurnosti ključno jest za uspješno provođenje ovih pravila. Korisnici trebaju biti dobro upoznati sa sigurnosnim aspektima pri korištenju računala i mjerama koje proizlaze iz njega, a to se potiče redovitom edukacijom. Potrebno je posebno voditi računa o edukaciji odgojitelja obzirom da oni rade u neposrednom radu s djecom.

Korisnici su obvezni čuvati podatke za pristup računalu tajnima. Nije dozvoljeno koristiti tuđe pristupne podatke pri korištenju računala. Ukoliko postoji potreba, obveza je traženje suglasnosti osobe čiji pristupni podaci se koriste. Nakon takvog korištenja, osoba čiji su se podaci koristili treba promijeniti svoje pristupne podatke.

U slučaju potrebe prosljeđivanja tuđe elektroničke pošte, poruku je potrebno proslijediti bez intervencije u sadržaj. Pri prosljeđivanju tuđe elektroničke pošte valja voditi brigu o zaštiti tuđih osobnih podataka.

Datoteke koje se preuzimaju iz vanjskog izvora mogu ugroziti sigurnost odgojitelja ili djece. Stoga je uputno ne otvarati ili prosljeđivati zaražene datoteke i programe kao ni otvarati datoteke iz nepoznatih ili neprovjerenih izvora. Sve takve datoteke valja najprije provjeriti antivirusnim alatom.

Pametni telefoni za vrijeme neposrednog rada odgojitelji mogu koristiti isključivo u svrhu provođenja pedagoškog rada (dokumentiranje procesa učenja djece, rad u eTwinning projektima i slično).

Politika prihvatljivog korištenja

Odgojitelje, stručne suradnike i djecu potiče se na korištenje informacijskih tehnologija i alata u svrhu unapređivanja pedagoške prakse.

Korisnici računala u Ustanovi dužni su ponašati se 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.

Djeca mogu raditi na računalu isključivo pod nadzorom odgojitelja. Odgojitelj je odgovoran za sadržaje koji su dostupni djetetu.

Roditelji ili skrbnici dobrovoljno potpisuju dozvolu za fotografiranje svojeg djeteta te dozvolu za objavljivanje fotografija djeteta u aktivnostima, a u svrhu predstavljanja pedagoške prakse. Za svaki

eTwinning projekt, roditelji djece uključene u isti, potpisuju dozvole za fotografiranje svojeg djeteta i objavljivanje fotografija djeteta u aktivnostima.

Prilikom objave na web stranicama Ustanove te ostalim web stranicama, nije dozvoljeno navoditi puno ime i prezime djeteta.

RAVNATELJICA:

Jasenska Husnjak, dipl. defektologinja