DJEČJI VRTIĆ POPOVAČA
Alojzija Stepinca 3, 44317 Popovača
Tel.: 044/ 679 - 034
mail: ravnateljica@vrtic-popovaca.hr | web: www.vrticpopovaca.hr

PRAVILNIK O INFORMACIJSKOJ SIGURNOSTI

SISAČKO-MOSLAVAČKA ŽUPANIJA

GRAD POPOVAČA

DJEČJI VRTIĆ POPOVAČA

listopad, 2026.

Na temelju odredbi Zakona o kibernetičkoj sigurnosti (Narodne novine, br. 14/24) i članka 50. Statuta Dječjeg vrtića Popovača (KLASA: 601-01/26-01/1, URBROJ: 2176-74-01-26-7), Upravno vijeće Dječjeg vrtića Popovača na 7. sjednici održanoj dana 21.10.2026. godine donosi

PRAVILNIK O INFORMACIJSKOJ SIGURNOSTI

I. OPĆE ODREDBE

Članak 1.

Ovim Pravilnikom o informacijskoj sigurnosti (u daljnjem tekstu: Pravilnik) utvrđuju se pravila, mjere i postupci za osiguranje informacijske sigurnosti u Dječjem vrtiću Popovača (u daljnjem tekstu: Vrtić). Svrha Pravilnika je zaštita informacijskog sustava, računalne opreme, mreže i podataka od neovlaštenog pristupa, izmjene, gubitka ili uništenja.

Članak 2.

Odredbe ovog Pravilnika obvezujuće su za sve zaposlenike Vrtića (odgojno-obrazovne djelatnike, administrativno-tehničko osoblje, stručni tim, ravnatelja/icu) te vanjske suradnike koji u svom radu koriste informacijsko-komunikacijsku opremu Vrtića ili imaju pristup podacima Vrtića.

II. UPRAVLJANJE RAČUNALNOM OPREMOM I MREŽOM

Članak 3.

Sva računalna i mrežna oprema (stolna i prijenosna računala, tableti, pisači, mrežni uređaji i dr.) vlasništvo su Vrtića i smiju se koristiti isključivo u poslovne svrhe, odnosno za potrebe provođenja programa i rada Vrtića.

Zabranjeno je samoinicijativno spajanje privatne računalne opreme na žičanu i zaštićenu bežičnu (Wi-Fi) mrežu Vrtića bez odobrenja ravnatelja/ice ili osobe zadužene za IT podršku.

Članak 4.

Zaposlenici su dužni pažljivo postupati s dodijeljenom opremom. Prilikom napuštanja radnog mjesta, zaposlenici su obvezni zaključati zaslon računala (kratica Windows + L ili odjava). Po završetku radnog vremena, sva računala i periferni uređaji moraju se sigurno ugasiti.

III. UPRAVLJANJE KORISNIČKIM RAČUNIMA I LOZINKAMA

Članak 5.

Pristup računalima i poslovnim aplikacijama dopušten je isključivo putem osobnih korisničkih računa. Svaki zaposlenik dobiva svoje korisničko ime i lozinku. Strogo je zabranjeno dijeljenje vlastitih lozinki s drugim zaposlenicima ili trećim osobama.

Članak 6.

Lozinke za pristup sustavu moraju biti složene i ispunjavati sljedeće minimalne uvjete:

*Sadržavati najmanje 8 znakova.

*Uključivati kombinaciju velikih i malih slova, brojeva i specijalnih znakova (npr. !, @, #, $, %).

*Lozinke se ne smiju zapisivati na papiriće (tzv. post-it listiće) i lijepiti na monitor ili radni stol.

*Promjena lozinke nužna je u slučaju sumnje da je kompromitirana, otkrivena neovlaštenim osobama ili da je došlo do sigurnosnog incidenta.

IV. SIGURNOST PODATAKA I KORIŠTENJE PRENOSIVIH MEDIJA

Članak 7.

Poslovni i osobni podaci o djeci, roditeljima/skrbnicima i zaposlenicima smiju se pohranjivati isključivo na lokalnim diskovima službenih računala Vrtića ili na službenom sigurnom poslužitelju (serveru/cloudu) Vrtića.

Članak 8.

Korištenje prenosivih medija (USB stickovi, vanjski tvrdi diskovi, memorijske kartice) dopušteno je samo za potrebe posla. Svi prenosivi mediji na kojima se prenose osobni ili povjerljivi podaci Vrtića moraju biti kriptirani (šifrirani) programskim rješenjem koje onemogućuje pristup podacima u slučaju gubitka ili krađe medija.

Članak 9.

Radi sprječavanja trajnog gubitka podataka uslijed kvara opreme ili kibernetičkih napada, Vrtić provodi redovitu izradu sigurnosnih kopija (backup) ključnih podataka (računovodstvo, tajništvo…). Sigurnosne kopije se pohranjuju na odvojenu lokaciju ili zaštićeni vanjski medij.

V. KORIŠTENJE INTERNETA I ELEKTRONIČKE POŠTE

Članak 10.

Službena elektronička pošta (e-mail adrese s domenom Vrtića ili službene adrese poput tajnica@vrtic-popovaca.hr) smije se koristiti isključivo za poslovnu komunikaciju.

Zaposlenici su dužni pokazati visok stupanj opreza pri otvaranju e-mail poruka od nepoznatih pošiljatelja, a osobito pri otvaranju privitaka (npr. .exe, .zip, .rar datoteke) ili klikanju na poveznice unutar sumnjivih poruka (opasnost od phishing napada).

Službena elektronička pošta koristi se isključivo za poslovnu komunikaciju, a zaposlenici su dužni:

*Redovito prazniti sandučić elektroničke pošte kako ne bi došlo do blokade primitka novih poruka.

*Prilikom masovnog slanja obavijesti roditeljima/skrbnicima obvezno koristiti polje „Skrivena kopija" (Bcc) kako e-mail adrese roditelja ne bi postale vidljive trećim stranama.

*Pokazati maksimalan oprez pri zaprimanju poruka od nepoznatih pošiljatelja koje zahtijevaju hitnu prijavu, unos lozinke ili potvrdu bankovnih podataka (phishing napadi). Takve poruke potrebno je odmah prijaviti Službeniku za zaštitu podataka (DPO).

Članak 11.

Zabranjeno je preuzimanje i instaliranje neovlaštenih, piratskih ili privatnih softvera i igara na službena računala Vrtića. Na računalima smiju biti instalirani samo licencirani programi odobreni od strane Vrtića. Sva računala moraju imati aktiviran i ažuriran antivirusni program.

Članak 11.a

Sva službena računala, poslužitelji i prijenosni uređaji Vrtića moraju imati instaliran, aktiviran i redovito ažuriran licencirani antivirusni program te aktiviran vatrozid (firewall).

U svrhu osiguranja stabilnosti sustava, zaposlenicima je strogo zabranjeno:

*samostalno isključivati, suspendirati ili mijenjati postavke antivirusnog programa,

*ignorirati upozorenja antivirusnog softvera o detektiranim prijetnjama ili zlonamjernim stranicama,

*spajati vanjske medije (USB stickove) na računalo ako antivirusni program signalizira prisutnost prijetnje.

Vrtić je dužan (putem ovlaštene IT podrške ili zadužene osobe) osigurati da se definicije virusa i sigurnosne zakrpe na svim operativnim sustavima ažuriraju automatski i bez odgađanja.

Ako antivirusni program detektira ozbiljnu ugrozu (crv, ransomware ili trojanski konj) koju ne može samostalno ukloniti, zaposlenik je dužan odmah postupiti sukladno odredbama članka 15. ovog Pravilnika (Postupanje u slučaju sigurnosnih incidenata).

Članak 12.

Službeni pristup internetu u Vrtiću namijenjen je isključivo za obavljanje poslovnih aktivnosti, stručno usavršavanje zaposlenika i provođenje odgojno-obrazovnog programa.

Zaposlenicima je strogo zabranjeno korištenje službene internetske mreže Vrtića za:

*Posjećivanje internetskih stranica s neprimjerenim, uvredljivim, pornografskim ili ilegalnim sadržajem.

*Preuzimanje velikih datoteka (filmovi, glazba, videoigre) koje nisu u vezi s radnim zadacima, a koje mogu preopteretiti ili usporiti računalnu mrežu Vrtića.

*Sudjelovanje u igrama na sreću (online kladionice i casina).

*Korištenje alata za neovlašteno dijeljenje datoteka (tzv. torrent protokoli).

Članak 13.

Prilikom korištenja privatnih profila na društvenim mrežama (Facebook, Instagram, TikTok, LinkedIn i dr.) unutar ili izvan radnog vremena, zaposlenici su dužni čuvati ugled Vrtića.

Strogo je zabranjeno na privatnim profilima društvenih mreža objavljivati fotografije, videozapise ili bilo koje druge podatke o djeci polaznicima Vrtića, kao i povjerljive informacije iz rada Vrtića (podaci o roditeljima, kolegama ili internim odlukama).

Strogo je zabranjeno, kako tijekom tako i izvan radnog vremena, na privatnim profilima društvenih mreža objavljivati:

• fotografije, videozapise ili audiozapise djece polaznika Vrtića,

• osobne podatke roditelja, skrbnika ili drugih zaposlenika Vrtića,

• interne informacije, dokumente ili odluke Vrtića.

Službene profile Vrtića na društvenim mrežama te službenu internetsku stranicu Vrtića smiju uređivati i na njima objavljivati sadržaj isključivo zaposlenici koje je za to pisanim putem ovlastio/la ravnatelj/ica, i to isključivo uz prethodno pribavljene pisane privole roditelja/skrbnika djece.

VI. POSTUPANJE U SLUČAJU SIGURNOSNIH INCIDENATA

Članak 14.

Informacijski sigurnosni incident je svaki događaj koji ugrožava povjerljivost, cjelovitost ili dostupnost podataka (npr. pojava računalnog virusa, zaključavanje ekrana od strane zlonamjernog softvera, gubitak USB sticka s podacima, neovlašteni ulazak u sustav).

Članak 15.

U slučaju uočavanja ili sumnje na sigurnosni incident, zaposlenik je dužan:

1. Odmah prekinuti rad na računalu i, po potrebi, isključiti uređaj s lokalne mreže (odspojiti mrežni kabel ili ugasiti Wi-Fi).

2. Bez odgađanja obavijestiti ravnatelja/icu Vrtića i Službenika za zaštitu osobnih podataka (DPO).

3. Ne poduzimati samostalne radnje brisanja ili popravka kako se ne bi uništili dokazi o incidentu.

Vrtić zadržava pravo da, u svrhu zaštite računalnog sustava od zlonamjernih softvera (virusa), tehnički blokira pristup određenim internetskim stranicama ili kategorijama sadržaja za koje se procijeni da predstavljaju sigurnosni rizik.

VII. ZAVRŠNE ODREDBE

Članak 16.

Nepoštivanje odredbi ovog Pravilnika od strane zaposlenika smatra se povredom obveza iz radnog odnosa u skladu sa Zakonom o radu i internim aktima Vrtića.

Članak 17.

Ovaj Pravilnik stupa na snagu osmoga dana od dana objave na oglasnoj ploči Dječjeg vrtića Popovača.

KLASA: 601-04/26-02/01

URBROJ: 2176-74-01-26-28

Popovača, 21. 10. 2026. godiňe

PREDSJEDNIK UPRAVNOG VIJEĆA

DJEČJI VRTIĆ POPOVAČA POPOVAČA

Zvonimir Bubalo

Pravilnik je objavljen na oglasnoj ploči dana 22. listopada 2026. godine.

Pravilnik stupa na snagu dana 30. listopada 2026. godine.

DJEČJI VRTIĆ POPOVAČA POPOVAČA A. Stepinca 3, Popovača

RAVNATELJICA

Andreja Zeman

Andreja Zeman, mag.praesc.educ.