Na podlagi Zakona o varstvu osebnih podatkov (ZVOP-1-UPB1, Ur. list RS št. 94/07) je ravnateljica Marjanca Vampelj (v nadaljevanju ustanova), **dne 29. 1. 2015** sprejela Pravilnik o varovanju osebnih in zaupnih podatkov.

PRAVILNIK O VAROVANJU OSEBNIH IN ZAUPNIH PODATKOV

I. SPLOŠNE DOLOČBE

1. člen

S tem pravilnikom se določajo organizacijski, tehnični in logistično-tehnični postopki in ukrepi za varovanje osebnih podatkov v ustanovi z namenom, da se prepreči slučajno ali namerno nepooblaščeno uničevanje podatkov, njihovo spremembo ali izgubo kakor tudi nepooblaščen dostop, obdelavo, uporabo ali posredovanje osebnih podatkov.
Delavci ustanove, ki pri svojem delu obdelujejo ali na kakršen koli način pridejo v stik z osebnimi podatki, morajo biti seznanjeni in pri delu spoštovati določbe Zakona o varstvu osebnih podatkov, področno zakonodajo, ki ureja področje njihovega dela ter vsebino tega pravilnika.

Z vsebino tega pravilnika morajo biti seznanjene tudi druge fizične osebe, ki so v delovnem ali drugem pogodbenem razmerju z ustanovo.

2. člen

V tem pravilniku uporabljeni izrazi imajo enak pomen, kot jim ga določa Zakon o varstvu osebnih podatkov (ZVOP-1; Uradni list RS, št. 94/2007-UPB1).
V nadaljevanju navedeni posamezni izrazi v ustanovi označujejo sledeče:

1. **Delavci** ustanove ali delavci – so npr. osebe, ki so v delovnem ali drugem pogodbenem razmerju z ustanovo in ki svoje storitve ali del le-teh opravljajo v prostorih oziroma na lokacijah ustanove ter so pogodbeno zavezani s spoštovanju določil tega pravilnika.

2. **Pooblaščenci** ustanove ali pooblaščenci – so osebe, ki so v delovnem ali drugem pogodbenem razmerju z ustanovo ter osebe podizvajalca ali drugega poslovnega partnerja ustanove, ki pri svojem delu obdelujejo osebne podatke oziroma zaradi dela pridejo na kakršen koli način v stik z osebnimi podatki, in so s strani ustanove pooblaščeni za obdelavo osebnih podatkov in pogodbeno zavezani k spoštovanju določil tega pravilnika.

3. **Osebni podatek** – je datum rojstva, matični indeks, podatek o oceni, naslov stalnega prebivališča, ipd.;

4. **Občutljiv osebni podatek** – je podatek o posebnih potrebah posameznika, podatek o morfoloških značilnostih posameznika, podatek o bolezenskem stanju in njegovem napredovanju, ipd.;

5. **Posameznik** – je učenec, učenka, dijak, dijakinja, starš, skrbnik, učitelj, strokovni delavec, zaposleni, ipd.;

6. **Upravljavec osebnih podatkov** – ustanova, ki vodi zbirke osebnih podatkov (Osnovna šola Vrhovci, Cesta na Bokalce 1, Ljubljana);

7. **Zbirka osebnih podatkov** – sta tudi npr. bazi podatkov informacijske rešitve eAsistent ter eAsistent za starše, v katerih so združeni osebni podatki za posameznega upravljavca osebnih podatkov;

8. **Nosilec podatkov** – so vse vrste sredstev, na katerih so zapisani ali posneti podatki, kot npr. listine, akti, gradiva, spisi, računalniška oprema vključno z magnetnimi, optičnimi ali drugimi računalniškimi mediji, fotokopije, zvočno in slikovno gradivo, mikrofilmi, naprave za prenos podatkov, ipd.;

9. **Obdelava osebnih podatkov** – je npr. storitev e-hrambe dokumentarnega gradiva ali nudenje uporabniške pomoči končnim uporabnikom, ki vključuje vpogled ali drugačen stik z osebnim/-i podatkom/-i posameznika ali dejanja programiranja in razvijanja informacijskih rešitev, za namene katerih je potreben dostop do osebnih podatkov in njihova obdelava, ipd.;

10. **Testni dostop** – dostop do dela informacijske rešitve, ki omogoča dostop do testnih podatkov, na katerih se osebni podatki predvidoma ne nahajajo.

11. **Administratorski dostop** – dostop do produkcijskega dela informacijske rešitve, ki omogoča dostop do osebnih podatkov, ki se obdelujejo za upravljavca osebnih podatkov ali naročnike, za namene zagotavljanja tehnične in splošne podpore, administracije ali programiranja in nadaljnjega razvoja informacijskih rešitev

Za varovane osebne podatke štejejo tisti podatki o fizični osebi, ki kažejo na lastnosti, stanja ali razmerja posameznika, ne glede na obliko, v kateri so izraženi.

3. člen

Varovanje osebnih podatkov zajema pravne, organizacijske in ustrezne logistično-tehnične postopke in ukrepe, s katerimi se:

- varujejo prostori, aparature in sistemska programska oprema;
- varuje aplikativna programska oprema, s katero se obdelujejo osebni podatki;
- zagotavlja varnost posredovanja in prenosa osebnih podatkov;
- onemogoča nepooblaščenim osebam dostop do naprav, na katerih se obdelujejo osebni podatki in do njihovih zbirk;
- zagotavlja učinkovit način blokiranja, uničenja, izbrisa ali anonimiziranja osebnih podatkov;
- omogoča poznejše ugotavljanje, kdaj so bili posamezni osebni podatki vneseni v zbirko osebnih podatkov, uporabljeni ali drugače obdelani in kdo je to storil, in

sicer za obdobje, ko je mogoče zakonsko varstvo pravice posameznika zaradi nedopustnega posredovanja ali obdelave osebnih podatkov.

4. člen

Obdelava in varovanje občutljivih osebnih podatkov, mora biti izvajana posebno vestno in skrbno.
Občutljivi osebni podatki morajo biti varovani tako, da se nepooblaščenim osebam prepreči dostop do njih.
Pri prenosu občutljivih osebnih podatkov preko telekomunikacijskih omrežij se šteje, da so podatki ustrezno zavarovani, če se posredujejo z uporabo kriptografskih metod in elektronskega podpisa tako, da je zagotovljena njihova nečitljivost oziroma neprepoznavnost med prenosom.

II. ODGOVORNE OSEBE TER ZAVEZANOST K VAROVANJU OSEBNIH PODATKOV

5. člen

Odgovorna oseba za pravilno izvajanje določb tega pravilnika je ravnateljica OŠ Vrhovci, Marjanca Vampelj.

Delavce ustanove se seznani z odgovorno osebo in tem pravilnikom ter izvajanjem določb.

6. člen

Vsi delavci ustanove, ne glede na to, ali pri svojem delu obdelujejo osebne podatke oziroma ali na kakršen koli način lahko pridejo v stik z osebnimi podatki, morajo biti seznanjeni z vsebino tega pravilnika in podpisati izjavo o varovanju osebnih podatkov, ki je lahko vključena tudi v določbe pogodbe ali Izjave in obrazce Notranjih pravil (v nadaljevanju NP).

Kot izjava o varovanju osebnih podatkov se lahko upošteva tudi veljavno sklenjeni sporazum o varovanju poslovnih skrivnosti (angleško NDA), v kolikor slednji vsebuje določbe o varovanju osebnih podatkov ter se sklicuje oziroma zavezuje k spoštovanju določil tega pravilnika.

Seznam oseb, ki so podpisale izjavo o varovanju osebnih podatkov oziroma NDA iz drugega odstavka tega člena je sestavni del Kataloga pooblastil (**NP – Katalog pooblastil**).

Vsak pooblaščenec ustanove mora ves čas skrbeti za varovanje osebnih podatkov, s katerimi pride v stik ali jih pri delu obdeluje, in jih ne sme spreminjati, urejati ali brisati brez predhodnega soglasja ravnatelja ustanove ali z njegove strani pooblaščene osebe, kakor tudi ne posredovati ali razkrivati nepooblaščenim osebam.

7. člen

Razume se, da pooblastilo predstavlja kakršen koli pravni akt z razporeditvijo delavca na ustrezno sistemizirano delovno mesto, za katerega so predvidena pooblastila vezana na določeno delovno mesto.

Ravnatelj ustanove ali z njegove strani njega pooblaščena oseba za področje informacijskih sistemov s pooblastilom, ki v praksi za potrebe informacijskih sistemov pomeni vpis odobrenih pooblastil v Katalog pooblastil, dovoljuje delavcu, da lahko za potrebe opravljanja svojega dela ob upoštevanju določb tega pravilnika in področne zakonodaje s področja šolstva oz. izobraževanja ali varstva osebnih podatkov pri svojem delu pride v stik z osebnimi podatki.

III. VAROVANJE PROSTOROV IN RAČUNALNIŠKE OPREME

Prostori, kjer se nahajajo osebni podatki

8. člen

Prostori, kjer se nahajajo osebni podatki, nosilci varovanih osebnih podatkov - vsak računalniški ali elektronski nosilec podatka, ali vsak dokument na katerem je zapisan osebni podatek in strojna ter programska oprema morajo biti varovani z organizacijskimi ukrepi, določenimi s tem pravilnikom, ki onemogočajo nepooblaščenim osebam dostop do podatkov.
Dostop do varovanih prostorov imajo le osebe, ki so pooblaščene s strani ravnatelja ali z njegove strani pooblaščene druge osebe in se vodijo v katalogu pooblastil, ki je sestavni del potrjenih Notranjih pravil. Na zavihku **– Evidence, Popis informacijskih virov ali namesto tega v drugih shemah in popisih** se vodi tudi evidenca prostorov, kjer se nahajajo osebni podatki, načini njihovega varovanja in seznam pooblaščenih oseb, ki imajo dostop do teh prostorov.

9. člen

V učilnice ali pisarne nezaposlene osebe ne smejo vstopati brez spremstva ali prisotnosti zaposlenega delavca. Delavec, ki dela v pisarnah, mora vestno in skrbno nadzorovati prostor ter vstope in izstope iz prostora in ob zapustitvi prostora zakleniti prostor.
Delavec, ki pri delu obdeluje osebne podatke, nosilcev osebnih podatkov ne sme puščati nenadzorovanih ali kako drugače izpostavljati nevarnosti vpogleda vanje nepooblaščenim osebam oziroma delavcem.
V prostorih, v katere imajo vstop stranke oziroma osebe, ki niso zaposlene v ustanovi, morajo biti nosilci podatkov in računalniški prikazovalniki nameščeni v času obdelave ali dela na njih tako, da je strankam onemogočen vpogled oz. dostop do osebnih podatkov. Nastavljeni morajo biti tudi ohranjevalniki zaslona za čas neaktivnosti delavca na računalniški opremi.

10. člen

Poslovni partnerji in drugi obiskovalci, se smejo gibati v prostorih ustanove le ob prisotnosti delavca ustanove, ki mora skrbeti za to, da bo dostop ali vpogled v nosilce podatkov nepooblaščenim osebam onemogočen. Prostori ustanove se morajo redno zaklepati, s čimer se nepooblaščenim osebam prepreči nenapovedan vstop.

11. člen

Tehnično-vzdrževalni delavci in čistilke se lahko gibljejo v varovanih prostorih izven delovnega časa in brez prisotnosti delavca le, če so nosilci osebnih podatkov shranjeni v zaklenjenih omarah ali arhivu (npr. ognjevarni sef), tehnično-vzdrževalni delavci in čistilke pa nimajo ključev teh omar ali arhivov oziroma so osebnih podatki shranjeni na zanje nedostopnih elektronskih medijih.

Tehnično osebje za vstop v ustanovo lahko uporablja svoje dostopno geslo na alarmni napravi (v kolikor obstaja), obenem se lahko izvaja videonadzor. Pri slednjem se morajo vsi posnetki periodično brisati najkasneje v 12 mesecih od dneva nastanka posnetka, če zakon ne določa drugače. O izvajanju videonadzora mora biti zagotovljeno vidno obvestilo skupaj s podatki izvajalca in njegovem kontaktu.

12. člen

Vstop v pisarne ustanove in učilnice

Za dostop do pisarne je potrebno imeti ključe pisarne. Za varovane prostore se priporoča tudi alarmna naprava. Ključe/kartice in dostopne kode razdelita ravnatelj ali druga odgovorna oseba po vpisu in podpisu IZJAVE o varovanju informacij delodajalca – ustanove in PROŠNJE za vzpostavitev ali dopolnitev pooblastil ter podeljene opreme s strani delavca. Dvojnike ključev pisarne je delavcem prepovedano izdelovati, razen v kolikor to ni izrecno naročeno delavcu s strani ravnatelja ustanove ali z njegove strani pooblaščene druge osebe.

Ključe pisarn se ne sme puščati v ključavnici v vratih iz zunanje ali notranje strani. Vhodna vrata se morajo, ob neprisotnosti vsaj enega delavca, sproti zaklepati.

Ključa/dostopne kartice ali vstopne alarmne kode delavec ne sme posojati ali dajati drugim osebam, niti v kolikor so to drugi delavci. V primeru izgube mora delavec nemudoma obvestiti odgovorno osebo, ki vodi in posodablja evidenco Kataloga pooblastil, ta pa mora izgubo in predvideni kraj in čas izgube evidentirati na poljuben način.

Način dostopanja v učilnice ustanova opredeli na način, ki ji zagotavlja ustrezno izvajanja izobraževalnega procesa.

Nosilci osebnih podatkov

13. člen

Nosilcev osebnih podatkov delavci ne smejo odnašati izven prostorov ustanove brez predhodnega dovoljenja ravnatelja. Ti nosilci podatkov so:

- vse izpolnjene obrazce in izjave (v kolikor le-te vsebujejo osebne podatke),
- arhivi, ki jih šole posredujejo na prenosnem mediju (CD/DVD),
- ostala dokumentacija, gradiva ali mediji, ki bi lahko vsebovali osebne podatke.

Ravnatelj lahko dovoli iznos nosilcev osebnih podatkov iz ustanove, ko predhodno delavec pojasni namen ter aktivnosti, vpiše namen in razlog za iznos podatkov iz

ustanove na **Evidenco o ravnanju z osebnimi podatki**. V primeru, da se podatkov ne iznaša, se taka evidenca ne vodi.

Kot iznos se ne šteje predaja osebnih podatkov pristojnim inštitucijam, ki se ga običajno vodi zapisniško.

Nosilce osebnih podatkov je potrebno po končanem delu ustrezno varovati oziroma zagotoviti nedostopnost.
V kolikor se nosilcev osebnih podatkov ne potrebuje več, jih je potrebno vrniti po priporočeni pošti upravljavcu osebnih podatkov in to zabeležiti v **Evidenco o ravnanju z osebnimi podatki**. V primeru, da se podatkov ne vrača, se taka evidenca ne vodi.

IV. VAROVANJE SISTEMSKE IN APLIKATIVNE RAČUNALNIŠKE OPREME TER PODATKOV, KI SE OBDELUJEJO Z RAČUNALNIŠKO OPREMO

14. člen

Dostop do računalniške programske opreme, kjer so shranjeni osebni podatki, ki jih ustanova uporablja, mora biti varovan na način, ki omogoča dostop samo pooblaščenim delavcem.

Računalniki ali strežniki, na katerih se obdelujejo osebni podatki, morajo biti ustrezno zaščiteni s sodobno antivirusno zaščito, imeti nameščen ohranjevalnik zaslona in nastavljeno omogočanje avtomatičnih popravkov operacijskega sistema.

Delavci oziroma pooblaščenci morajo upoštevati vsa interna navodila ravnatelja ali informatika v zvezi z računalniško opremo in temu primerno strežnike in računalnike tudi uporabljati.

15. člen

Odgovorna oseba ustanove (informatik) oziroma druga pooblaščena oseba mora skrbeti, da se v primeru servisiranja, popravila, spreminjanja ali dopolnjevanja sistemske ali aplikativne programske opreme z osebnimi podatki ob morebitnem kopiranju osebnih podatkov, po prenehanju potrebe po kopiji, kopija uniči.

Odgovorna oseba ustanove (informatik) oziroma druga pooblaščena oseba mora biti v času servisiranja računalniške opreme in programske opreme z osebnimi podatki v prostorih ustanove ves čas prisoten in mora nadzirati, da ne pride do nedopustnega ravnanja z osebnimi podatki, zlasti v primeru, če se na računalniški opremi nahajajo podatki, ki uživajo posebno varstvo po tem pravilniku ali po Zakonu o varstvu osebnih podatkov.

16. člen

Vzdrževanje in popravilo strojne računalniške in druge opreme, s katero se obdelujejo osebni podatki, je dovoljeno samo z vednostjo in odobritvijo ravnatelja oziroma informatika ali druge pooblaščene osebe.

Vsaka oseba, ki izvaja vzdrževanje in popravilo strojne računalniške in druge opreme z nameščenimi osebnimi podatki, v kolikor ne gre za pooblaščenca ustanove, je dolžna podati Izjavo o varovanju osebnih podatkov, razen v kolikor ni vsebina izjave vključena v pogodbo ali Dogovor o obveznosti varovanja podatkov, sklenjeno med in izvajalcem vzdrževanja ali popravila strojne računalniške in druge opreme oziroma drug ustrezen dogovor.

17. člen

V primeru, če se izkaže potreba po popravilu računalniške opreme, kjer se nahajajo osebni podatki, izven ustanove, brez kontrole pooblaščenega delavca ustanove in pri osebah, ki ne podpišejo dogovorov o varovanju osebnih podatkov, se morajo osebni podatki iz diska računalnika izbrisati na način, ki onemogoča restavracijo. Če tak izbris ni mogoč pa se iz računalnika nosilci podatkov, za čas popravila, predvidoma odstranijo

18. člen

Ob pojavu računalniškega virusa ali sumu na takšen pojav je potrebno storiti vse, da se obvesti informatika, ki samostojno ali s pomočjo strokovnjakov virus odpravi oziroma prepreči in da se ugotovi vzrok pojava virusa.
Vsi podatki in programska oprema, ki so namenjeni uporabi na računalnikih ustanove in v računalniškem informacijskem sistemu ter prispejo v ustanove na medijih za prenos računalniških podatkov ali prek telekomunikacijskih kanalov, morajo biti pred uporabo preverjeni glede prisotnosti računalniških virusov z antivirusnim programom.

O morebitnem pojavu računalniškega virusa, je delavec, ki je zaznal takšen pojav, dolžan ravnati skladno s Politiko upravljanja varnostnih incidentov ter izpolniti predvideno **poročilo (identifikacija varnostnega incidenta) kot to določajo NP, PrilogaF.**

19. člen

Shranjevanje osebnih podatkov na računalnike, ki niso namenjeni za opravljanje dela v ustanovi ni dovoljeno.

Delavec, ki osebne podatke shranjuje na tak računalnik je materialno in kazensko odgovoren, v kolikor bi prišlo do razkritja osebnih podatkov, ki se obdelujejo v ustanovi.

20. člen

Za službeno opremo se štejejo računalniki, ki so locirani v poslovnih prostorih ustanove se evidentirajo v Evidenci osnovnih sredstev.

Delavec z nastopom dela in podpisom Izjave o varstvu osebnih podatkov, lahko po odobritvi ravnatelja prenosni računalnik uporablja tudi za delo na domu ali na terenu.

Ravnatelj določi Informatika ali drugo pooblaščeno osebo za vodenje Kataloga pooblastil.

21. člen

Dostop do podatkov vseh uporabljanih informacijskih rešitev, e-storitev in druge službene opreme mora biti zavarovan z geslom skladno z določili NP.

Gesla je potrebno redno spreminjati oziroma tudi ob vsakem sumu, da je prišlo do zlorabe gesla. Novo geslo ne sme biti enako ali podobno prejšnjemu.

22. člen

Gesel za dostop do sistemske in aplikativne računalniške opreme ter gesla za dostop do eAsistenta, eHrambe drugih e-storitev in ostalih informacijskih rešitev, ki jih delavec uporablja za delo, se ne sme shranjevati na papirju ali na način, da je dostop do gesel omogočen brez zahteve po vpisu gesla ali pa so gesla shranjena v ognjevarnem arhivu/sefu (predvidoma za administratorska gesla).

V primeru zlorabe gesla ali suma zlorabe gesla, je potrebno geslo nemudoma spremeniti, nato pa o zlorabi gesla ali sumu zlorabe gesla obvestiti informatika ali drugo pooblaščeno osebo. O zlorabi gesla ali sumu zlorabe gesla informatik izpolni **poročilo (Identifikacija varnostnega incidenta)**.

POOBLASTILA ZA DOSTOP DO INFORMACIJSKIH REŠITEV OZIROMA E-STORITEV

23. člen

Delavcu, ki pri svojem delu nujno potrebuje dostop do informacijskih rešitev in e-storitev in ki v okviru izpolnjevanja delovnih obveznosti opravlja tudi dejanja, ki pomenijo obdelavo osebnih podatkov upravljavca osebnih podatkov, odgovorna oseba ustanove (predvidoma informatik) dodeli dostop na podlagi izpolnjenega, podpisanega in s strani ravnatelja potrjenega obrazca za podelitev pooblastil.

Dostop do osebnih podatkov iz prejšnjega odstavka tega člena je lahko omejen ali neomejen ter se loči na:

a) testni uporabnik – uporabnik z dostopom do testnega okolja,
b) uporabnik – običajen uporabnik,
b) administrator – administrator v posamezni informacijski rešitvi.

Za delavce oziroma pooblaščence, ki pridobijo bodisi omejen ali neomejen dostop do podatkov, veljajo določila tega pravilnika v celoti in se zanje uporablja izraz delavec, pooblaščenec ali administrator.

Odgovorna oseba vodi evidenco vseh izdanih in preklicanih pooblastil. Evidenca se lahko vodi v Katalogu pooblastil.

24. člen

Delavec, ki ima administratorski dostop do informacijske rešitve mora pri delu z osebnimi in zaupnimi podatki ravnati še posebej skrbno, da se ne razkrijejo osebni podatki nepooblaščeni osebi ali razkrijejo zaupni podatki, ki se štejejo za poslovno skrivnost naročnikov.

25. člen

Delavec samovoljno ne sme nikoli posredovati svojega uporabniškega imena in gesla za administratorski dostop nepooblaščeni osebi, nadrejenemu ali sodelavcu/-ki, izjema je le daljša odsotnost, ko je dostop do določenih vsebin njuno potreben za nemoteno poslovanje zavoda.

Razkritje uporabniškega imena in gesla drugi osebi bi lahko pomenilo zelo resne kršitve 93. člena Zakona o varstvu osebnih podatkov (ZVOP-1), v kolikor bi prišlo do razkritja osebnih podatkov, ki se varujejo v skladu s tem Pravilnikom ter hudo kršitev delovnega razmerja, ki lahko predstavlja razlog za odpoved pogodbe o zaposlitvi ter odškodninske zahteve.

26. člen

Geslo za administratorski dostop informacijskih rešitev in e-storitev mora ustrezati Politiki gesel ustanove. Njegove lastnosti (dolžina, pogostost obnavljanja, druge lastnosti gesel, ipd.) za informacijske rešitve ali e-storitve, iz katerih se ustvarjajo gradiva, se naj upravljajo avtomatično.

27. člen

Odgovorna oseba lahko administratorski dostop delavcu ali pooblaščencu ustanove tudi odvzame začasno ali trajno. Vzroki za odvzem pooblastila so sledeči:

- prenehanje delovnega razmerja ali drugega pogodbenega razmerja, na podlagi katerega je bil dostop dodeljen,
- prenehanje opravljanja del, ki zahtevajo administratorski dostop,
- kršitve ali sum na kršitve določb tega pravilnika.

Odgovorna oseba odvzame administratorski dostop delavcu ali pooblaščencu ustanove s preklicem pooblastila ali z njegovo zamrznitvijo.

V. STORITVE, KI JIH OPRAVLJAJO ZUNANJE PRAVNE ALI FIZIČNE OSEBE

28. člen

Z vsako zunanjo pravno ali fizično osebo, ki opravlja posamezna opravila v zvezi z zbiranjem, obdelovanjem, shranjevanjem ali posredovanjem osebnih podatkov kot del informacijskih rešitev in e-storitev in je registrirana za opravljanje takšne dejavnosti (zunanji pooblaščenec ali pogodbeni obdelovalec), se sklene pisna pogodba o obdelovanju osebnih podatkov.

V pogodbi ali v dodatku k pogodbi morajo biti obvezno predpisani tudi pogoji in ukrepi za zagotovitev varstva osebnih podatkov in njihovega zavarovanja in na kakšen način

lahko ustanova izvaja kontrolo nad varstvom osebnih podatkov. Pogodba se lahko sklicuje tudi na določbe tega pravilnika ali posebnega akta, ki vsebuje takšna navodila.

Pooblaščena pravna ali fizična oseba, ki za ustanove opravlja dogovorjene storitve izven prostorov upravljavca, mora imeti vsaj enako strog način varovanja osebnih podatkov, kakor ga predvideva ta pravilnik.

VI. SPREJEM IN POSREDOVANJE OSEBNIH PODATKOV

29. člen

Delavec ali pooblaščenec, ki je pooblaščen za sprejem in evidenco pošte, odpira in pregleduje vse poštne pošiljke in pošiljke, ki na drug način prispejo na ustanovo.

Delavec, ki je zadolžen za sprejem in evidenco pošte, ne odpira tistih pošiljk, ki so naslovljene na drug organ ali organizacijo in so pomotoma dostavljena ter pošiljk, ki so označene kot osebni podatki. Takšno poštno pošiljko mora predati pravemu naslovniku, ravnatelju ustanove, ali drugi osebi, ki jo ravnatelj v ta namen pooblasti, oziroma ravnati po njenem navodilu.

Delavec ali pooblaščenec, ki je zadolžen za sprejem in evidenco pošte, ne sme odpirati pošiljk, naslovljenih na delavca, na katerih je na ovojnici navedeno, da se vročijo osebno naslovniku, ter pošiljk, na katerih je najprej navedeno osebno ime delavca brez označbe njegovega uradnega položaja in šele nato naslov ustanove. Ta določba se ne uporablja v primeru podeljenega izrecnega pooblastila za vročanje poštnih pošiljk določene vrste.

30. člen

Osebne podatke je dovoljeno prenašati z informacijskimi, telekomunikacijskimi in drugimi sredstvi le ob izvajanju postopkov in ukrepov, določenimi s tem pravilnikom in drugimi internimi akti, ki nepooblaščenim osebam preprečujejo prilaščanje ali uničenje podatkov ter neupravičeno seznanjanje z njihovo vsebino.

Občutljivi osebni podatki se pošiljajo naslovnikom v zaprtih ovojnicah proti podpisu v dostavni knjigi ali z vročilnico ali preko varnih informacijskih povezav (HTTPS, SSL, SSH, kriptirana epošta).

Osebni podatki in vsi dokumenti, ki vsebujejo osebne podatke, se pošiljajo po priporočeni pošti s povratnico. Vse prejete povratnice se hranijo vsaj 3 leta.

Ovojnica, v kateri se posredujejo osebni podatki, mora biti izdelana na takšen način, da ovojnica ne omogoča, da bi bila ob normalni svetlobi ali pri osvetlitvi ovojnic z običajno lučjo vidna vsebina ovojnice. Prav tako mora ovojnica zagotoviti, da odprtja ovojnice in seznanitve z njeno vsebino ni mogoče opraviti brez vidne sledi odpiranja ovojnice.

31. člen

Obdelava občutljivih osebnih podatkov mora biti posebej označena in zavarovana.

Podatki iz prejšnjega odstavka se smejo posredovati upravičenim osebam preko telekomunikacijskih omrežij samo, če so posebej zavarovani s kriptografskimi metodami in elektronskim podpisom tako, da je zagotovljena nečitljivost podatkov med njihovim prenosom.

32. člen

Osebni podatki se posredujejo samo tistim uporabnikom, ki se izkažejo z ustrezno zakonsko podlago ali s pisno zahtevo oziroma privolitvijo posameznika, na katerega se podatki nanašajo.

Za vsako posredovanje osebnih podatkov mora upravičenec vložiti pisno vlogo, v kateri mora biti jasno navedena določba zakona, ki uporabnika pooblašča za pridobitev osebnih podatkov, ali pa mora k vlogi priložena pisna zahteva oziroma privolitev posameznika, na katerega se podatki nanašajo.

Nikoli se ne posredujejo originali dokumentov, razen v primeru pisne odredbe sodišča. Originalni dokument se mora v času odsotnosti nadomestiti s kopijo, na kateri se navede, kje se nahaja original ter kdaj je bil original posredovan oz. kopija narejena.

VII. BRISANJE PODATKOV

33. člen

Osebni podatki se lahko vodijo v zbirki osebnih podatkov, če se jo vodi, le toliko časa, kolikor je potrebno, da se doseže namen, za katerega se zbirajo in vodijo. Metapodatkovni podatki eHrambe se štejejo in vodijo kot zbirke osebnih podatkov le v primeru in od prejema mnenja odgovornega organa, ki tak status potrdi, dalje.

Brisanje osebnih podatkov se lahko izvaja le skladno z veljavno zakonodajo in le v kolikor pooblaščenec razpolaga z dovoljenjem upravljavca osebnih podatkov za brisanje.

Po prenehanju potrebe po vodenju osebnih podatkov, se podatki in vse kopije podatkov zbrišejo oziroma uničijo. Vsi izbrisi oz. vsa uničenja se evidentirajo v **evidenci o izbrisu osebnih podatkov in kopij osebnih podatkov kot to določajo NP.**

Arhivsko gradivo se ne sme brisati oziroma se predaja in odbira kot to določajo Navodila za odbiranja prejeta s strani pristojnega arhiva.

Metapodatki in vsi z njimi povezani podatki, ki so osnova za vpoklic dokumentov o posamezniku, se vodijo ves čas do predaje gradiv pristojnim arhivom ne glede na določila ZVOP-1 o prenehanju namena zbiranja osebnih podatkov, saj v nasprotnem primeru ni mogoča enolična informacijska uparitev oseb in z njimi povezanih dokumentov, ki jih je izdala ustanova.

34. člen

Brisanje osebnih podatkov na računalniških medijih in drugih nosilcih osebnih podatkov se opravi na način, po postopku in metodi, ki onemogoča restavriranje brisanih podatkov.

Osebni podatki, vsebovani na klasičnih nosilcih (listine, kartoteke, register, seznam) se brišejo z uničenjem nosilcev. Nosilci se fizično uničijo (razrežejo) v prostorih ustanove ali pod nadzorom pooblaščenega delavca ustanove pri organizaciji, ki se ukvarja z uničevanjem zaupne dokumentacije.

Osebni podatki, vsebovani na računalniških medijih (trdi diski, USB ključki,...) se predvideno brišejo z namensko programsko opremo za brisanje podatkov. V ta namen se lahko uporabi tudi brezplačno dostopno programsko opremo kot je npr. CC cleaner, DBAN, ipd..

Ko računalniški mediji niso več uporabni, se morajo trajno uničiti. Trajno uničenje se zapiše v evidenco o izločanju ali uničenju nosilcev podatkov.

35. člen

Z vso vestnostjo in skrbnostjo, določeno s tem pravilnikom, se mora brisati in uničevati tudi pomožna dokumentacija ali računalniški produkti oziroma predloge, ki vsebujejo posamezne osebne podatke.

Uničevanje osebnih podatkov na nosilcih iz predhodnega odstavka se mora izvajati tekoče in ažurno.

VIII. UKREPANJE OB UGOTOVITVI ZLORABE OSEBNIH PODATKOV ALI VDORU V ZBIRKE OSEBNIH PODATKOV

36. člen

Delavci ustanove so dolžni izvajati ukrepe za preprečevanje zlorabe osebnih podatkov in morajo z osebnimi podatki, s katerimi se seznanijo pri svojem delu, ravnati vestno in skrbno na način in po postopkih, ki jih določa ta pravilnik ter v skladu s predpisi, ki urejajo to področje.
Delavec, ki izve ali opazi, da je prišlo do zlorabe osebnih podatkov (nepooblaščen vpogled v osebne podatke, odkrivanje osebnih podatkov, nepooblaščeno uničenje, nepooblaščeno spreminjanje, poškodovanje zbirke, prilaščanje osebnih podatkov) ali do vdora v zbirko osebnih podatkov, mora takoj zagotoviti ukrepe za zaščito podatkov in o tem nemudoma obvestiti ravnatelja ali drugo pooblaščeno odgovorno osebo, ki morata poskrbeti, da se zaustavi nadaljnja zloraba osebnih podatkov ter zavaruje dokaze. O vdoru ali kakšnem drugem informacijskem varnostnem incidentu je delavec skupaj s pooblaščeno odgovorno osebo (informatik) dolžan izpolniti **Poročilo (identifikacija varnostnega incidenta)** in ga predložiti ravnatelju.

37. člen

Za zlorabo osebnih podatkov se šteje vsaka uporaba osebnih podatkov v namene, ki niso v skladu z namenom zbiranja, določenim v zakonu in medsebojni pogodbi z upravljavcem osebnih podatkov ali pogodbo o poslovnem sodelovanju s podizvajalcem

ali drugim poslovnim partnerjem, na podlagi katere se le-ti zbirajo ali namenom določenem v katalogu zbirk osebnih podatkov, v kolikor se le-ta prijavi na urad Informacijske pooblaščenke. Za poskus zlorabe šteje poskus uporabe osebnih podatkov v nedovoljene namene. Ravnatelj mora zoper tistega, ki je zlorabil osebne podatke ali je nepooblaščeno vdrl v zbirko osebnih podatkov, ustrezno ukrepati.

IX. ODGOVORNOST ZA IZVAJANJE UKREPOV ZAVAROVANJA OSEBNIH PODATKOV

38. člen

Pred nastopom dela delavca na delovnem mestu, kjer se zbirajo, urejajo, obdelujejo, spreminjajo, shranjujejo, posredujejo ali uporabljajo osebni podatki ali nosilci osebnih podatkov, mora delavec podpisati izjavo, ki ga zavezuje k varovanju osebnih podatkov kot poklicne skrivnosti in ki ga opozarja na posledice kršitve zaveze (lahko gre za samostojno izjavo ali člen v pogodbi).

Obveza varovanja osebnih podatkov, s katerimi se delavec seznani pri svojem delu v ustanovi, traja tudi po prenehanju delovnega razmerja v ustanovi za neomejeno ali v naprej opredeljeno obdobje.

39. člen

Delavec, ki je pooblaščen za obdelavo osebnih podatkov upravljavca osebnih podatkov, je dolžan spoštovati določbe tega pravilnika.
V primeru kršitev določb tega pravilnika ali področne zakonodaje, prekoračitve ali zlorabe danega mu pooblastila ali v primeru, da pri izpolnjevanju svojih delovnih obveznosti ne potrebuje več dostopa do osebnih podatkov upravljavca osebnih podatkov, je odgovorna oseba dolžna nemudoma preklicati izdano pooblastilo in odvzeti vsa gesla, s katerimi je dostopal do teh podatkov. V primeru suma zgoraj navedenih kršitev ali suma zlorabe pooblastila, sme odgovorna oseba brez predhodnega opozorila začasno odvzeti pooblastila in preprečiti uporabo gesel.

40. člen

Delavec stori lažjo kršitev delovne dolžnosti:

- če opusti vestno in skrbno nadzorovanje varovanih prostorov,
- če opusti ravnanja za preprečitev vpogleda v ali na nosilce osebnih podatkov,
- če ne uniči kopije osebnih podatkov v primerih iz 3. odst. 33. člena,
- če ni ves čas servisiranja računalnika in programske opreme v prostorih ustanove prisoten, če se v računalniku nahajajo podatki, ki uživajo posebno varstvo po tem pravilniku ali po Zakonu o varstvu osebnih podatkov,
- če ne izvaja preventive v zvezi z računalniškimi virusi in
- če ne obvesti ravnatelja ali pooblaščenega delavca v primeru zlorabe osebnih podatkov ali vdora v zbirko osebnih podatkov, v kolikor le-to vodi.

41. člen

Delavec stori hujšo kršitev delovne dolžnosti:

- če zbira, uporabi ali posreduje osebne podatke v nasprotju z zakonom,

- če krši dolžnost varovanja zaupnosti podatkov in dokumentov ustanove in njenih naročnikov,
- če ne dopolni evidence o ravnanju z osebnimi podatki o posredovanju osebnih podatkov institucijam,
- če namenoma popravlja, spreminja ali dopolnjuje sistemsko ali aplikativno programsko opremo brez vednosti odgovorne osebe in na način, ki lahko privede do razkritja osebnih podatkov,
- če ni pooblaščen za inštalacijo programske opreme na službeno opremo in to izvede brez izrecnega dovoljenja ravnatelja ali od njega pooblaščene osebe,
- če redno ne izdeluje kopije vsebine osebnih podatkov shranjenih izven informacijskih rešitev in e-storitev, v kolikor se kopije ne izdelujejo avtomatično ter ne hrani računalniških kopij vsebin zbirk osebnih podatkov na računalniku, ki ga uporablja, na ustrezen način.

42. člen

O zlorabi ali sumu zlorabe osebnih podatkov, vodenih v zbirkah osebnih podatkov ustanove, s strani oseb, ki niso delavci ustanove, ravnatelj ustanove ali z njegove strani pooblaščena oseba obvesti organe pooblaščene za pregon.

Poslovna skrivnost in varovanje dokumentov, ki vsebujejo poslovne skrivnosti

43. člen

Vsi dokumenti in podatki, ki zadevajo organizacijo in poslovanje ustanove, zaposlene v ustanovi, naročnike, njihovo poslovanje in poslovne odnose s ustanovo, se varujejo kot poslovna skrivnost.

Drugače lahko za posamezne dokumente in podatke odloči ravnatelj ustanove. Razkrivanje takih podatkov tretjim osebam brez pisnega dovoljenja ravnatelja, ki ni pogojeno z opravljanjem delovnih nalog, pomeni kršitev delovnih obveznosti in posledično disciplinsko ter odškodninsko odgovornost kršitelja.

Nihče od zaposlenih v ustanovi, ki nima od ravnatelja za to pisnega predhodnega dovoljenja, razen prokurista, ni pooblaščen za dajanje kakršnih koli podatkov ali dokumentov ustanove, zaposlenih ali strank tretjim osebam, medijem ali uradnim organom.

X. PRILOGE K PRAVILNIKU

44. člen

Ta pravilnik uporablja priloge, ki so sestavni del potrjenih Notranjih pravil in vsebujejo:

a) Evidence (zapisi v Katalogu pooblastil)
- Evidenca pooblaščencev (poleg vodstva ustanove), ki skrbijo za pravilno izvajanje določb pravilnika
- Evidenca prostorov, če se v njih nahajajo OP
- Evidenca o ravnanju z osebnimi podatki v primeru servisiranja ali popravila opreme
- Evidenca o varnostnih incidentov (evidenca se pripravi ob prvem tovrstnem primeru)
- Evidenca o osnovnih sredstvih
- Evidenca o izbrisu osebnih podatkov in kopij osebnih podatkov (evidenca se pripravi ob prvem tovrstnem primeru)

b) Katalog pooblastil tudi s podatki naslednjih Seznamih:
- Seznam oseb, ki so podpisale Izjavo o varovanju osebnih podatkov oz. prilagojen NDA
- Seznam oseb, ki imajo dostop do prostorov, kjer se nahajajo OP
- Seznam oseb, ki so prejele dostopne kode in ključ pisarne
- Seznam oseb, ki so prejemnik službene opreme

c) Obrazci
- Izjave vodstva in zaposlenih o varovanju osebnih podatkov
- Obrazec za podelitev pooblastil in opreme

d) Druge evidence
- Evidenca o predaji podatkov zunanjim institucijam (evidenca se pripravi in oblikuje ob prvem tovrstnem posredovanju).

45. člen

Ravnatelj ustanove hrani evidence ali določi drugo odgovorno osebo, pri kateri se hranijo te evidence oziroma osebe, ki so dolžne skrbeti za ažurno vodenje evidenc.

Oseba, zadolžena za vodenje ali/in hrambo posameznih evidenc, sme le-te združevati in povezovati med seboj in jih voditi na poljuben način.

PREHODNE IN KONČNE DOLOČBE

46. člen

Spremembe in dopolnitve tega pravilnika določi ravnatelj.

47. člen

Delavec s podpisom pogodbe o zaposlitvi ali ustrezne Izjave potrjuje, da je seznanjen in soglaša z vsemi določbami tega pravilnika.

Šteje se, da je delavec seznanjen z določbami novega pravilnika z dnem prejema tega pravilnika, pri čemer ima prejem v elektronski obliki enak pomen kot prejem tega pravilnika v papirnati obliki.

Ustanova je vsakemu delavcu dolžna zagotoviti lastno kopijo ali omogočiti vpogled v zadnjo veljavno verzijo pravilnika.

48. člen

S sprejetjem tega pravilnika preneha veljati Pravilnik o zbiranju in varstvu osebnih podatkov v Osnovni šoli Vrhovci od 2. junija 2006.

Ljubljana, 29. 1. 2015
Številka:

Ravnateljica
Marjanca Vampelj