PATVIRTINTA
Vilniaus lopšelio darželio „Pelėda“
direktoriaus
2025 m. spalio 27 d. įsakymu Nr. V-151

VILNIAUS LOPŠELIO-DARŽELIO „PELĖDA“ INFORMACINIŲ IR KOMUNIKACINIŲ TECHNOLOGIJŲ NAUDOJIMO BEI DARBUOTOJŲ STEBĖSENOS IR KONTROLĖS DARBO VIETOJE TVARKOS APRAŠAS

I. BENDROSIOS NUOSTATOS

1. Informacinių ir komunikacinių technologijų (toliau – IKT) naudojimo bei darbuotojų stebėsenos ir kontrolės darbo vietoje tvarkos aprašas (toliau – Aprašas) nustato Vilniaus lopšelio-darželio „Pelėda“ (toliau – Įstaiga) IKT naudojimo darbo vietoje principus, darbuotojų stebėsenos ir kontrolės tvarką, apimtį ir sąlygas.

2. Šiame Apraše vartojamos sąvokos:

2.1. **Informacinės ir komunikacinės technologijos** – Įstaigos veikloje naudojami elektroninių ryšių tinklai, kompiuteriai, mobilieji ir stacionarūs prietaisai, fiksuotojo ir mobiliojo ryšio įranga, kompiuterių programos, dokumentų valdymo sistemos, duomenų saugojimo ir perdavimo priemonės, prieiga prie interneto, elektroninio pašto sistemos ir kita techninė bei programinė įranga, skirta informacijai rinkti, įrašyti, saugoti, kaupti, apdoroti, perduoti ar kitaip tvarkyti.

2.2. **Naudotojas** – Įstaigos darbuotojas, naudojantis Įstaigos IKT priemones darbo funkcijoms vykdyti.

2.3. **IT administratorius** – Įstaigos darbuotojas, atsakingas už IKT sistemų priežiūrą, administravimą, saugumą ir techninę pagalbą.

2.4. **Darbuotojų stebėsena** – Įstaigos vykdomas darbuotojų veiklos stebėjimas darbo vietoje, naudojant technines ar programines priemones (pvz., prieigos registrus, el. pašto srautų analizę, vaizdo stebėjimą), siekiant užtikrinti darbo organizavimo, saugumo, turto apsaugos ir teisės aktų laikymosi kontrolę.

2.5. **Kontrolė** – Įstaigos atliekami veiksmai, skirti patikrinti, ar darbuotojai laikosi nustatytų darbo, saugos, informacijos saugumo ir IKT naudojimo taisyklių.

2.6. **Asmens duomenys** – bet kokia informacija apie fizinį asmenį, kurio tapatybė yra nustatyta arba gali būti nustatyta tiesiogiai ar netiesiogiai, visų pirma pagal identifikatorių, kaip vardą, pavardę, asmens kodą, buvimo vietos duomenis, interneto identifikatorių ar kitus požymius.

2.7. **Duomenų tvarkymas** – bet koks su asmens duomenimis atliekamas veiksmas ar veiksmų rinkinys, toks kaip rinkimas, įrašymas, saugojimas, keitimas, naudojimas, perdavimas, skleidimas, naikinimas ar kitaip tvarkymas.

3. Apraše vartojamos sąvokos yra parengtos vadovaujantis galiojančiais Europos Sąjungos ir Lietuvos Respublikos teisės aktais, įskaitant, bet neapsiribojant, Bendruoju duomenų apsaugos reglamentu (ES) 2016/679, Lietuvos Respublikos darbo kodeksu ir Asmens duomenų teisinės apsaugos įstatymu. Prireikus, sąvokos gali būti aiškinamos atsižvelgiant į šių teisės aktų nuostatas ir Įstaigos veiklos specifiką.

II. INFORMACINIŲ IR KOMUNIKACINIŲ TECHNOLOGIJŲ NAUDOJIMAS

4. Įstaiga, atsižvelgdama į darbuotojo einamas pareigas ir darbo funkcijas, savo nuožiūra suteikia darbo priemones: kompiuterį, mobilųjį telefoną, prieigą prie interneto, elektroninio pašto paskyrą, dokumentų valdymo sistemą ir kitą informacinių bei komunikacinių technologijų įrangą, reikalingą darbo funkcijoms vykdyti.

5. Suteiktos IKT priemonės išlieka Įstaigos nuosavybe ir yra skirtos išimtinai darbo funkcijoms vykdyti. Jų naudojimas asmeniniams (privatiems) poreikiams yra draudžiamas, nebent su darbuotoju susitarta kitaip, rašytiniu Įstaigos vadovo sprendimu.

6. Draudžiama naudoti Įstaigos IKT:

6.1. veiklai, nesusijusiai su darbo funkcijų atlikimu;

6.2. Įstaigos veiklai, interesams ar reputacijai pakenkti;

6.3. informacijai skleisti ar laikyti, kuria kurstomas smurtas, tautinė, rasinė, religinė ar socialinė neapykanta, platinama pornografija, propaguojamos ar reklamuojamos seksualinės paslaugos, narkotinės ar psichotropinės medžiagos;

6.4. komerciniais, asmeniniais ar neteisėtais tikslais, taip pat šmeižiančiai, įžeidžiančiai, grasinančiai ar dorovei prieštaraujančiai informacijai skleisti, kompiuterių virusams siųsti ar kitai veiklai, pažeidžiančiai Įstaigos ar kitų asmenų teisėtus interesus;

6.5. pažeidžiant trečiųjų asmenų intelektinės nuosavybės teises;

6.6. įsibrovimui į kitas IKT sistemas;

6.7. nepageidaujamiems elektroniniams pranešimams (spam) siųsti;

6.8. kitai veiklai, kuri prieštarauja galiojantiems teisės aktams, Įstaigos vidaus dokumentams ar bendriesiems etikos principams.

7. Naudotojams draudžiama kurti, siųsti, saugoti, kaupti ar naudoti su darbu nesusijusią grafinę, garso ar vaizdo medžiagą, žaidimus, programinę įrangą, taip pat siųsti failus, užkrėstus virusais ar kitais kenksmingais programiniais kodais, galinčiais sutrikdyti kompiuterinių ar telekomunikacinių įrenginių bei programinės įrangos veikimą ir saugumą.

8. Įstaigos IKT priemonės gali būti naudojamos tik su tinkamai licencijuota programine įranga. Draudžiama diegti, saugoti, naudoti, kopijuoti ar platinti neautorizuotą, neteisėtą, autorines teises pažeidžiančią ar asmeninę programinę įrangą.

9. Naudotojai privalo laikytis Įstaigos vadovo ir (ar) IT administratoriaus nurodymų dėl asmens duomenų, konfidencialios informacijos ir kitų jautrių duomenų siuntimo, saugojimo, tvarkymo bei apsaugos.

10. Naudotojams draudžiama savavališkai keisti IKT sistemos ar jos atskirų resursų nustatymus, parametrus, naudoti kitus prisijungimo būdus ir priemones, ardyti ar modifikuoti kompiuterius ar kitą techninę įrangą, taip pat atlikti bet kokius veiksmus, galinčius neigiamai paveikti IKT sistemų veikimą, saugumą ar stabilumą.

11. Draudžiama naudoti Įstaigos IKT neteisėtai prieigai prie duomenų ar sistemų, jų saugumo tikrinimui, skenavimui, tinklo srauto stebėjimui ar kitai veiklai, kuri gali pažeisti informacijos saugumą ir konfidencialumą.

12. Prieš naudojant išorines laikmenas (pvz., USB atmintines, išorinius kietuosius diskus, SD korteles, CD/DVD ar kitus duomenų kaupiklius), jose esantys duomenys turi būti patikrinti kompiuteryje instaliuota antivirusine programa, siekiant užtikrinti Įstaigos IKT saugumą.

13. Elektroninio pašto, kurį suteikia Įstaiga, naudojimui taikomi šie pagrindiniai reikalavimai:

13.1. elektroninis paštas naudojamas tik darbo funkcijoms vykdyti;

13.2. naudotojai, besinaudojantys Įstaigos elektroniniu paštu, atstovauja Įstaigą, todėl privalo elgtis atsakingai ir saugoti Įstaigos reputaciją;

13.3. su darbo funkcijų atlikimu susiję gauti ir išsiųsti elektroninio pašto pranešimai turi būti archyvuojami naudotojo kompiuteryje arba kitoje Įstaigos vadovo ir (ar) IT administratoriaus nurodytoje vietoje;

13.4. jei naudotojas nesinaudoja elektroniniu paštu ilgiau nei vieną darbo dieną (pvz., dėl atostogų, komandiruotės, ligos ar kt.), jis privalo aktyvuoti automatinį atsakymą, informuojantį siuntėjus apie laikiną nedalyvavimą.

14. Žiniatinklio naudojimui taikomi šie pagrindiniai reikalavimai:

14.1. žiniatinklis naudojamas tik darbo funkcijoms vykdyti;

14.2. draudžiama lankytis pornografinio, smurtinio, azartinių lošimų ar kito abejotino turinio svetainėse;

14.3. be Įstaigos vadovo ir (ar) IT administratoriaus leidimo draudžiama registruotis žiniatinklio svetainėse ar skelbti jose informaciją, susijusią su Įstaiga ar jos veikla.

15. Naudotojai privalo laikytis šiame Apraše nustatytų IKT naudojimo taisyklių. Pažeidus šias taisykles, gali būti taikomos Darbo kodekse ir kituose teisės aktuose numatytos drausminės atsakomybės priemonės.

III. SAUGUMO PRIEMONĖS

16. Įstaigos IKT resursų naudotojai privalo laikytis šio Aprašo, taip pat kitų Įstaigos vidaus taisyklių, instrukcijų ir Įstaigos vadovo bei (ar) IT administratoriaus nurodymų, susijusių su IKT naudojimu. Jei naudotojui kyla abejonių dėl tam tikrų veiksmų teisėtumo ar tinkamumo, prieš juos atlikdamas jis privalo pasikonsultuoti su Įstaigos vadovu ir (ar) IT administratoriumi.

17. Kiekvienas naudotojas prie Įstaigos IKT sistemos jungiasi naudodamasis jam suteiktu slaptažodžiu ar kitais autentifikavimo duomenimis.

18. Naudotojai privalo saugoti savo slaptažodžius ir autentifikavimo duomenis, jų neatskleisti kitiems darbuotojams ar tretiesiems asmenims. Jei slaptažodis tampa žinomas kitiems asmenims, naudotojas privalo jį nedelsdamas pakeisti.

19. Būtina laikytis Įstaigos vadovo ir (ar) IT administratoriaus nurodymų dėl slaptažodžių sudarymo, keitimo periodiškumo ir kitų saugumo reikalavimų. Slaptažodžiai turi būti ne trumpesni nei 12 simbolių, sudaryti iš didžiųjų ir mažųjų raidžių, skaičių ir specialiųjų simbolių, būti unikalūs ir nenaudojami kitose darbuotojo naudojamose sistemose ar įrenginiuose.

20. Draudžiama naudotis kito naudotojo prisijungimo duomenimis ar prisijungti prie kito darbuotojo paskyros, net jei prieiga techniškai įmanoma. Tokie veiksmai laikomi saugumo pažeidimu ir gali būti vertinami kaip drausmės pažeidimas, už kurį taikoma atsakomybė pagal galiojančius teisės aktus ir Įstaigos vidaus dokumentus.

21. Naudotojams draudžiama leisti tretiesiems asmenims naudotis Įstaigos IKT resursais. Jie privalo imtis visų įmanomų priemonių, kad apsaugotų IKT nuo neteisėtos prieigos.

22. Pastebėję IKT sistemų sutrikimus ar bandymus trikdyti jų veikimą, naudotojai privalo nedelsdami informuoti Įstaigos vadovą ir (ar) IT administratorių bei užregistruoti incidentą pagal Įstaigoje nustatytą tvarką.

23. Naudotojai privalo taikyti būtinas atsargumo priemones, kad apsaugotų Įstaigos IKT nuo kompiuterių virusų ir įsilaužimų. Kilus įtarimui dėl saugumo pažeidimo, naudotojas turi nedelsdamas nutraukti darbą ir informuoti atsakingus asmenis.

24. Draudžiama išjungti ar keisti antivirusinės apsaugos priemonių veikimą Įstaigos IKT įrenginiuose.

25. Naudotojai privalo dalyvauti Įstaigos organizuojamuose mokymuose ar instruktažuose, susijusiuose su saugiu IKT naudojimu ir kibernetiniu saugumu.

26.Pasibaigus darbo santykiams su Įstaiga, naudotojas netenka teisės naudotis Įstaigos IKT resursais.

IV. STEBĖSENA IR KONTROLĖ DARBO VIETOJE

27. Įstaiga organizuoja darbo vietoje vykdomos elektroninės ar kitokios komunikacijos stebėseną, kai tai būtina profesinės veiklos užtikrinimui, Įstaigos turto, informacinių sistemų ar konfidencialios informacijos apsaugai. Tam tikrais atvejais stebėsena gali apimti ir asmeninės ar kitokios informacijos srautų valdymą, jei tai susiję su darbo funkcijų vykdymu.

28. Stebėsena vykdoma vadovaujantis proporcingumo principu – ji taikoma tik tada, kai siekiamų tikslų negalima pasiekti kitomis, mažiau darbuotojų privatumą ribojančiomis priemonėmis. Įstaiga užtikrina, kad stebėsena būtų būtina, tinkama ir neperteklinė, atitinkanti teisėtą Įstaigos interesą, kaip numatyta BDAR 6 straipsnio 1 dalies f punkte.

29. Stebėsenos ir kontrolės darbo vietoje tikslai:

29.1. apsaugoti Įstaigos konfidencialią informaciją nuo atskleidimo tretiesiems asmenims;

29.2. apsaugoti Įstaigos klientų ir darbuotojų asmens duomenis nuo neteisėto perdavimo, atskleidimo ar panaudojimo tretiesiems asmenims;

29.3. apsaugoti Įstaigos informacines sistemas (IKT) nuo įsilaužimų, duomenų vagysčių, virusų, kenkėjiškų programų ir pavojingų interneto svetainių;

29.4. apsaugoti Įstaigos turtą ir užtikrinti asmenų saugumą Įstaigos patalpose ir teritorijoje;

29.5. apsaugoti Įstaigos turtinius interesus ir užtikrinti darbuotojų darbo pareigų vykdymą.

30. Įstaiga, vykdydama darbuotojų stebėseną, vadovaujasi šiais principais:

30.1. būtinumo principas – stebėsenos priemonės taikomos tik tada, kai jos yra neišvengiamai būtinos siekiant nustatytų tikslų. Prieš taikydama bet kokią kontrolės formą, Įstaiga įsitikina, kad ji yra būtina ir negali būti pakeista mažiau intervencine alternatyva;

30.2. tikslingumo principas – duomenys renkami aiškiam, konkrečiam ir teisėtam tikslui, ir nėra tvarkomi nesuderinamais tikslais;

30.3. skaidrumo principas – Įstaigoje draudžiamas paslėptas stebėjimas (pvz., vaizdo, elektroninio pašto, interneto naudojimo), išskyrus atvejus, kai tai leidžiama pagal įstatymus arba būtina siekiant nustatyti pažeidimus darbo vietoje;

30.4. proporcingumo principas – renkami tik tie duomenys, kurie yra būtini ir nepertekliniai, atsižvelgiant į siekiamą tikslą;

30.5. tikslumo ir saugojimo trukmės principas – duomenys turi būti tikslūs, prireikus atnaujinami, ir saugomi ne ilgiau, nei būtina pagal nustatytą tikslą.

30.6. saugumo principas – Įstaiga taiko technines ir organizacines priemones, užtikrinančias, kad duomenys būtų apsaugoti nuo neteisėtos prieigos, praradimo ar kitokio pažeidimo.

31. Įstaigoje, siekiant šiame Apraše nurodytų tikslų, naudojamos specialios programos, kurios automatiškai registruoja darbuotojų interneto naršymo istoriją. Šie duomenys saugomi

vienerius metus. Jie nėra nuolat stebimi – peržiūrimi tik esant pagrįstam įtarimui dėl teisės aktų ar darbo pareigų pažeidimo, ir tik tiek, kiek būtina galimam pažeidimui ištirti. Pasibaigus saugojimo laikotarpiui, duomenys turi būti saugiai sunaikinami, vadovaujantis BDAR 5 straipsnio nuostatomis.

32. Darbuotojai iš anksto informuojami, kad Įstaiga gali tikrinti jiems priskirtuose kompiuteriuose įdiegtų komunikacijos programų (pvz., „Microsoft Teams“, „Outlook“, „Slack“) turinį ar kitą elektroninį susirašinėjimą, tiek, kiek tai būtina šio Aprašo numatytiems tikslams pasiekti, laikantis Apraše nurodytų principų.

33. Įstaiga pasilieka teisę be atskiro įspėjimo riboti prieigą prie tam tikrų interneto svetainių ar programinės įrangos. Jei šių priemonių nepakanka, Įstaiga gali tikrinti, kaip darbuotojas laikosi elektroninio pašto ir interneto naudojimo taisyklių, tirti incidentus, o esant poreikiui – perduoti darbuotojo naudotą įrangą tyrimui tretiesiems asmenims, turintiems teisę gauti tokius duomenis pagal teisės aktus.

34. Įstaiga, iš anksto informavusi darbuotojus, gali įrengti vaizdo stebėjimo įrenginius Įstaigos patalpose ar teritorijoje, siekdama Apraše nurodytų tikslų, laikydamasi Apraše išdėstytų principų bei vadovaudamasi Asmens duomenų teisinės apsaugos įstatymu. Vaizdo stebėjimas taikomas tik esant objektyviai būtinybei, kai tai būtina Įstaigos turto, asmenų ar informacijos saugumui užtikrinti. Stebėjimas nėra skirtas nuolatinei vaikų ar darbuotojų veiklos kontrolei, todėl kamerų įrengimas vaikų grupėse nėra taikomas kaip įprasta ar prevencinė priemonė.

35. Esant poreikiui ir iš anksto informavusi darbuotojus, Įstaiga gali taikyti ir papildomas stebėsenos priemones (pvz., garso įrašymą, transporto priemonių vietos nustatymą), jei tai būtina siekiant stebėsenos tikslų, nurodytų šiame skyriuje, ir laikantis nustatytų duomenų apsaugos bei proporcingumo principų.

36. Įstaiga užtikrina, kad darbuotojai būtų aiškiai ir iš anksto informuoti apie taikomas stebėsenos priemones, jų tikslus, apimtį, duomenų saugojimo trukmę ir galimą duomenų perdavimą tretiesiems asmenims.

37. Darbuotojai turi teisę kreiptis į Įstaigos vadovą ar IT administratorių dėl stebėsenos priemonių paaiškinimo ar duomenų tvarkymo klausimų.

V. BAIGIAMOSIOS NUOSTATOS

38. Šis Aprašas yra privalomas visiems Įstaigos darbuotojams, kurie naudojasi Įstaigos informacinėmis ir komunikacinėmis technologijomis.

39. Darbuotojai su Aprašu ir jo pakeitimais supažindinami pasirašytinai, naudojant šio Aprašo priedą Nr. 1.

40. Šio Aprašo pažeidimas, atsižvelgiant į pažeidimo pobūdį ir (ar) jo pasekmes, gali būti laikomas šiurkščiu darbo pareigų pažeidimu, už kurį gali būti taikoma drausminė atsakomybė, įskaitant darbo sutarties nutraukimą pagal Lietuvos Respublikos darbo kodekso 58 straipsnį.

41. Jei Įstaigoje dirba vidutiniškai 20 ir daugiau darbuotojų, apie šio Aprašo priėmimą ir/ar jo pakeitimus darbo taryba yra informuojama, vadovaujantis Lietuvos Respublikos darbo kodekso 206 straipsnio nuostatomis. Konsultavimasis vykdomas prieš priimant sprendimus, susijusius su darbuotojų stebėsena, kontrolės priemonėmis, informacinių ir komunikacinių technologijų naudojimu darbo vietoje.

42. Jeigu darbo taryba Įstaigoje nesudaryta, informavimas ir konsultavimas vykdomas su darbuotojų patikėtiniu arba darbdavio lygmeniu veikiančia profesine sąjunga, jei tokia yra.

43. Jeigu tam tikri klausimai šiame Apraše nėra reglamentuoti, jie sprendžiami vadovaujantis galiojančiais Lietuvos Respublikos teisės aktais, įskaitant, bet neapsiribojant, Darbo kodeksu, Asmens duomenų teisinės apsaugos įstatymu ir Bendruoju duomenų apsaugos reglamentu (BDAR).