PATVIRTINTA

Vilniaus technologijų mokymo centro

direktoriaus 2020 m. kovo 30 d.

įsakymu Nr. V1-144

**VILNIAUS TECHNOLOGIJŲ MOKYMO CENTRO MOKYMO NUOTOLINIU BŪDU**

**ASMENS DUOMENŲ APSAUGOS TVARKA**

1. **SKYRIUS**

**BENDROSIOS NUOSTATOS**

1. Vilniaus technologijų mokymo centro (toliau - Centro) mokymo nutoliniu būdu asmens duomenų apsaugos tvarka (toliau – Tvarka) aprašo Centro nuotolinio mokymo aplinką komunikuojant mokytojams ir mokiniams, prisijungimą prie jos, siekiant užtikrinti asmens duomenų saugumą virtualioje aplinkoje.
2. Ši Tvarka parengta atsižvelgiant į Nacionalinio kibernetinio saugumo centro bazines kibernetinio saugumo rekomendacijas nuotoliniam darbui.
3. Ši Tvarka papildo ir galioja kartu su Centro asmens duomenų tvarkymo taisyklėmis, Mokymo nuotoliniu būdu taisyklėmis, Centro asmens duomenų tvarkymo politika ir jos įgyvendinimo tvarkos aprašu.

**II SKYRIUS**

**DARBO APLINKA**

4. Nuotoliniam mokymui Centre naudojamos mokymo aplinkos:

4.1. elektroninis dienynas „Mano dienynas“ (pranešimams mokiniams/tėvams, namų darbų/užduočių skyrimui, mokinių vertinimui);

4.2. virtuali mokymosi aplinka „Microsoft Office 365 Teams“ (komunikacijai ir bendravimui klasėje/grupėje žinutėmis, nuotolinėms sinchroninėms pamokoms, interaktyvioms telekonferencijoms);

4.3. Microsoft Office elektroninis paštas .

**III SKYRIUS**

**PRISIJUNGIMAS**

5. Visiems dirbantiems nuotolinio mokymo aplinkoje (mokiniams ir mokytojams) suteikiami asmeniniai prisijungimo duomenys prie virtualios mokymosi aplinkos (Microsoft Office 365 Teams ir Mano dienynas):

5.1. Mokiniams sukurtus prisijungimo duomenis perduoda grupės vadovas (kuratorius), asmeniškai nusiųsdamas prisijungimus kiekvienam mokiniui atskirai.

5.2. Darbuotojams prisijungimus pateikia IT administratorius (IT specialistas).

5.3. Bendrojo ugdymo programą besimokančių mokinių tėvams duomenis pateikia el. dienyno administratorius.

6. Prisijungimo duomenis draudžiama saugoti el. laikmenose, laisvai prieinamose, matomose vietose. Draudžiama prisijungimo duomenis perduoti tretiesiems asmenims.

**IV SKYRIUS**

**REIKALAVIMAI ASMENS DUOMENŲ IR TEISIŲ APSAUGAI**

7. Siekiant nepažeisti asmens teisių, apsaugoti jų garbę ir orumą, renkant ir viešai skelbiant informaciją, mokiniams draudžiama:

7.1. filmuoti, fotografuoti mokytojus, vedančius nuotolines sinchronines pamokas;

7.2. daryti pamokų garso ir vaizdo įrašus, juos platinti.

.

8. Siekiant nepažeisti mokinių asmens duomenų apsaugos teisių, mokytojai negali viešai skelbti mokinių pasiekimų, pažymių, drausminių priemonių, kontaktinių duomenų, informacijos apie pažangą, nes šie duomenys yra laikytini asmens duomenimis, jei iš jų galima nustatyti asmens tapatybę, (pavyzdžiui, jei yra nurodomas pažymys ir jį gavusio mokinio vardas ir pavardė), todėl mokytojai tvarkant konkretaus mokinio pasiekimus šiuos duomenis turi nuasmeninti. Apibendrinti grupės pasiekimų rezultatai (pavyzdžiui grupės pažangumo vidurkis, nėra laikomi asmeniniais duomenimis ir asmens duomenų teisės apsaugos įstatymas netaikomas).

9. Siekiant nepažeisti autorinių teisių mokytojai, rengiantys medžiagą nuotoliniam mokymui, kai skaitmenina tekstinę, vaizdinę ar kitokią medžiagą, į kurią autorinių teisių neturi, gali atgaminti, viešai paskelbti ir viešai rodyti nedidelius teisėtai išleistus ar viešai paskelbtus kūrinius ir trumpas teisėtai išleistų ar viešai paskelbtų kūrinių ištraukas tiek originalo kalba, tiek išverstus į kitą kalbą, kiek tai susiję su mokymo programomis ir neviršija mokymui reikalingo masto, nurodant autorius ir šaltinius (pagal APA reikalavimus).

10. Siekiant apsaugoti asmens duomenis, mokiniai ir mokytojai turi saugiai dirbti internete:

10.1. Centro įrenginiai prie informacinių išteklių turėtų jungtis tik saugiu būdu. Privalu įsitikinti, kad naršyklės adreso juostoje būtų matomas https (saugus protokolas). Darbuotojai ir mokiniai iš namų turi jungtis tik iš žinomų įrenginių, naudojant prisijungimo vardą ir unikalų slaptažodį;

10.2. nuotoliniu būdu prie mokymosi aplinkų ir kitų informacinių išteklių jungtis naudojant tik legalią operacinę sistemą ir kitą programinę įrangą;

10.3. naudoti legalią antivirusinę programinę įrangą, rekomenduojama su papildomu funkcionalumu – ugniasiene, elektroninio pašto apsauga ir pan. Periodiškai atlikti kompiuterio skenavimus dėl kenkėjiškos programinės įrangos;

10.4. atidžiai vertinti nuorodas elektroniniuose laiškuose, nuolat tikrinti siunčiamos informacijos patikimumą, nepriiminėti skubotų sprendimų;

10.5 įsitikinti, ar kompiuteryje ir į tinklą prijungtuose įrenginiuose naudojama programinė įranga yra naujausios versijos, ar įdiegti programinės įrangos atnaujinimai (jeigu ne – atsisiųsti ir įdiegti);

10.6. Perduodamą keliamą jautrią informaciją (pvz. naudojantis debesijos paslaugomis) apsaugoti slaptažodžiais, kurie būtų perduodami kitais būdais (pvz. SMS žinutėmis.)

**V SKYRIUS**

**BAIGIAMOSIOS NUOSTATOS**

11. Nuotoliniu būdu dirbantis ar besimokantis asmuo prisiima atsakomybę už šios Tvarkos nuostatų ir rekomendacijų laikymąsi.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_