

Jelgavā

APSTIPRINĀTS
Jelgavas Mūzikas vidusskolas
direktors Artūrs Puķītis

2019. gada 23. augustā

Jelgavas Mūzikas vidusskolas Informācijas sistēmas lietošanas noteikumi

I. Vispārīgie jautājumi

1. Informācijas sistēmas lietošanas noteikumus nosaka Jelgavas Mūzikas vidusskolas (turpmāk – Iestāde) darbinieku pienākumus un prasības Iestādes izmantotās informācijas sistēmas un interneta lietošanai, kā arī nosaka kārtību, kādā tiek veikta Iestādes izmantotās informācijas sistēmas lietotāju pieejas tiesību piešķiršana, izmaiņas un anulēšana.
2. Noteikumos lietotie termini:
 - 2.1. **Informācijas sistēma** – strukturizēts informācijas tehnoloģiju un datu bāzu kopums, kuru lietojot tiek nodrošināta Iestādes izpildei nepieciešamās informācijas ierosināšana, radīšana, apkopošana, uzkrāšana, apstrādāšana, izmantošana un iznīcināšana.
 - 2.2. **Jelgavas Mūzikas vidusskola** – Iestāde, kas normatīvajos aktos noteiktajā kārtībā organizē un vada informācijas sistēmu darbību.
 - 2.3. **Informācijas sistēmas lietotājs** – persona, kurai ir piešķirtas piekļuves tiesības informācijas sistēmās.
 - 2.4. **IT speciālists** – Iestādes vai ārpalpojuma darbinieki, kā arī Kultūras ministrijas Informācijas un tehnoloģiju atbalsta nodaļas speciālisti, kuri Iestādes normatīvajos aktos noteiktā kārtībā veic nepieciešamos datortehnikas apkalpošanas darbus. Ārpalpojuma gadījumā veicamo darbu apjomu un pienākumus nosaka ārpalpojuma sniedzēja līguma nosacījumi.
3. Informācijas sistēmas lietošanas noteikumi ir saistoši visiem Iestādes darbiniekiem (pilna darba laika, nepilnas slodzes un līgumdarbiniekiem), kuri ir nodarbināti Iestādē un kam ir piekļuve kādai no Iestādes informācijas sistēmām.
4. Katra Iestādes Informācijas sistēmas lietotāja pienākums ir iepazīties ar šiem noteikumiem un ievērot tos ikdienas darbā.

II. Informācijas sistēmas lietotāju administrēšanas kārtība

5. Iestādes direktors ir atbildīgs par sev un to padotībā esošo darbinieku lietotāju pieejas tiesību piešķiršanu, izmaiņu veikšanu un anulēšanu.

6. Lai Iestādes lietojamām ārējām informācijas sistēmām izveidotu lietotāju pieejas tiesības vai veiktu izmaiņas tajās, Iestādes direktors raksta pieprasījumu vai rīkojumu (1.Pielikums), atzīmējot tajā nepieciešamo Informācijas resursu. Sastādītais pieprasījums (rīkojums) tiek nosūtīts direktora parakstīts pieprasījums informācijas sistēmas uzturētājam. Iekšējo informācijas sistēmu pieejas tiesību piešķiršanai Lietotājam, Iestādes direktors norīko IT speciālistu attiecīgo piekļuves tiesību piešķiršanai, bet nepieciešamības gadījumā sastāda arī pieprasījumu vai rīkojumu (1.Pielikums).
7. Informācijas sistēmas lietotāju pieejas tiesības tiek piešķirtas Iestādes darbiniekiem atbilstoši katra atsevišķā darbinieka noteiktajiem darba pienākumiem un specifikai.
8. Informācijas sistēmas uzturētājs izskata lietotāju pieejas tiesību piešķiršanas pieprasījumu un izveido (piešķir) atbilstošās informācijas sistēmas lietošanas tiesības un nosūta (nodod) tās Lietotājam.
9. Informācijas sistēmas lietotāju pieejas tiesību piešķiršana Iestādes informācijas resursiem personām, kuras nav Iestādes darbinieki, notiek tikai atsevišķos gadījumos pēc direktora vai IT speciālista pieprasījuma (piemēram, gadījumā ja ir noslēgts līgums starp Iestādi un atbilstošo personu, kurā ir precīzi noteikti personas pienākumi, pieļaujamie informācijas izmantošanas mērķi, konfidencialitātes prasības un atbildība).
10. IT speciālists ir atbildīgs par Iestādes iekšējo informācijas sistēmu Lietotāju pieejas tiesību izveidošanu, administrēšanu un šo pieprasījumu apkopošanu, glabāšanu, kontroli un uzraudzību. IT speciālists nodrošina kontroli un sniedz konsultācijas Iestādes direktoram, lai novērstu iespējamo risku neatbilstošo pieejas tiesību piešķiršanai visām Iestādē izmantojamajās sistēmās.
11. Piešķirtās lietotāju pieejas tiesības Iestādes informācijas resursiem ir nekavējoties jāanulē šādos gadījumos:
 - 11.1. darbiniekiem, kuri pārtrauc darba (līguma) tiesiskās attiecības ar Iestādi un / vai tās vairs nav nepieciešamas pienākumu veikšanai;
 - 11.2. personām, kuras ir izpildījušas savstarpēji noslēgto līgumu ar Iestādi vai šī līguma izbeigšanās (atcelšanas) gadījumā.
12. Iestājoties šo noteikumu 11.punktā minētajam gadījumam, Iestādes direktoram, kura pakļautībā ir iepriekš minētais darbinieks, Iestādes direktoram ir pienākums anulēt attiecīgā Lietotāja piekļuves tiesības, par ko sastāda pieprasījumu, saskaņā ar 6.punktu, kurā norāda par attiecīgā Lietotāja pieejas tiesību anulēšanas nepieciešamību.
13. Piešķirtās lietotāju pieejas tiesības var anulēt IT speciālists, balstoties uz atbilstošā lietotāja Informācijas sistēmas drošības politikas vai to saistošo dokumentu pārskatītiem, par to rakstiski informējot Iestādes direktoru.
14. IT speciālistam pēc Iestādes direktora pieprasījuma, ir pienākums sagatavot Lietotāju pieejas tiesību sarakstu, ja nepieciešams – norādot piekļuves līmeni.
15. IT speciālistam ir pienākums vismaz reizi gadā veikt Lietotāju pieejas tiesību kontroli, pārbaudot un salīdzinot piešķirto lietotāju pieejas tiesību atbilstību darbinieka (personas, kuras darbojas uz līguma pamata) pienākumiem un specifikai.

III. Informācijas sistēmas lietotāju tiesības, pienākumi un atbildība

16. Informācijas sistēmas lietotājam ir tiesības izmantot viņam lietošanā nodotos datorus un to programmatūru, kā arī Informācijas sistēmas lietotājam ir tiesības pieprasīt atbalstu gadījumā, ja datoram vai tā programmatūrai ir radušies traucējumi.

17. Informācijas sistēmas lietotājs ir atbildīgs par datortehniku, kas nodota viņa rīcībā, kā arī atbild par darbībām, kas tiek veiktas ar viņam nodoto datortehniku.
18. Informācijas sistēmas lietotājs nedrīkst atļaut piekļūt tam nodotai datortechnikai citām personām, ja tas nav nepieciešams tiešo darba pienākumu pildīšanai un to pilnvarojumu nav devis Iestādes direktors vai IT speciālists.
19. Informācijas sistēmas lietotāja pienākums ir apzināti nepieļaut datorvīrusu iekļūšanu iestādes datorsistēmās un neizmantojot nezināmas izcelsmes datu nesējus. Rodoties aizdomām, ka dators ir inficēts ar datorvīrusu, par to nekavējoties jāinformē IT speciālists.
20. Informācijas sistēmas lietotājam ir pienākums jebkuru ienākošo elektronisko informāciju (failus) pirms lietošanas obligāti pārbaudīt ar antivīrusa programmatūru, ja tas netiek nodrošināts automātiski.
21. Nelicencētas programmatūras uzstādīšana un lietošana darba stacijās (lietotāja datoros) ir aizliegta. Patvaļīgi uzstādītas programmatūras lietošana, bez Iestādes direktora vai IT speciālista atļaujas ir aizliegta.
22. Informācijas sistēmas lietotājs nedrīkst izpaust nepilnvarotām personām ziņas par Iestādes datoru tīkla uzbūvi un konfigurāciju.
23. Informācijas sistēmas lietotājs nedrīkst no sava darba datora kopēt failus uz ārējiem datu nesējiem (piemēram, CD, DVD, USB kartēm vai citiem datu nesējiem), ja to nevajag tiešo darba pienākumu pildīšanai vai ja tam pilnvarojumu nav devis Iestādes direktors vai IT speciālists.
24. Ārējo datu nesēju, kurā ir iekopēta ierobežotas pieejamības informācija, no Iestādes telpām drīkst iznest tikai ar Iestādes direktora RAKSTISKU atļauju. Šajos gadījumos Informācijas sistēmas lietotājs, kurš no iestādes telpām iznes šādu datu nesēju, uzņemas pilnu materiālo atbildību par šo informāciju un radītajiem zaudējumiem – datu noplūdei.
25. Informācijas sistēmas lietotājam ir aizliegts patvaļīgi pārvietot, demontēt aparatūru, izjaukt, remontēt iekārtas vai veikt citas darbības, kas varētu traucēt informācijas un tehnisko resursu darbību.
26. Informācijas sistēmas lietotājam ir aizliegts veikt paroļu minēšanu, drošības ievainojamības pārbaudes, kodēto datu atkodēšanu, izmantot noklausīšanās programmas un veikt citas darbības, kas vērstas uz informācijas un tehnisko resursu drošības vājināšanu.

IV. Interneta un e-pasta lietošana

27. Pieeju Internetam darbiniekiem piešķir vienlaicīgi ar Informācijas sistēmas lietotāja pieejas tiesībām Iestādes datortīklam (domēnam), kas nepieciešams, lai nodrošinātu iestādes darbību un klientiem sniegtos pakalpojumus.
28. Informācijas sistēmas lietotājam darba vajadzībām ir jāizmanto tikai Iestādes piešķirtais e-pasts.
29. Informācijas sistēmas lietotājam ir aizliegts, izmantojot Iestādes piešķirto e-pastu, reģistrēties dažādos interneta resursos, kas tiek izmantoti privātām vajadzībām.

30. Informācijas sistēmas lietotājam ir aizliegts atvērt e-pasta pielikumus vai atvērt sūtījumā iekļautās Interneta adreses, kas saņemtas no nenoskaidrotiem sūtītājiem, vai ir pamatotas aizdomas, ka e-pasts var saturēt kaitniecisku programmatūru pielikumā esošajos failos.

31. Lietojot Internetu, darbinieki pārstāv Iestādi un tie ir atbildīgi, lai Internets tiktu izmantots darba vajadzībām ētiski un atbilstoši normatīvo aktu prasībām.

32. Darbiniekiem, izmantojot e-pastu, ir jānodrošina, ka visas komunikācijas tiek veiktas profesionālām vajadzībām un netraucē pašu darbinieku darba produktivitāti, kā arī netiek izplatīta vai sūtīta informācija, kas ir aizsargāta ar autortiesībām. Iestāde no darbinieka ir tiesīga piedzīt zaudējumus, kas Iestādei var būt radušies, maksājot atlīdzību autortiesību īpašniekam par autortiesību pārkāpumu.

33. Darbinieki ir atbildīgi par visu nosūtīto tekstuālo, audio un vizuālo saturu. IT speciālists bez saskaņošanas ar darbinieku patur sev tiesības pārlūkot darbinieku saņemto un nosūtīto e-pastu saturu, ja uzskata to par nepieciešamu. Piekļuvi pie Iestādes darbinieku elektroniskā pasta IT speciālists nodrošina saskaņā ar Iestādes direktora vai tiesībsargājošu institūciju pieprasījumu.

34. IT speciālistam ir tiesības bloķēt atsevišķu interneta resursu izmantošanu, kā arī ir tiesības piekļūt Informācijas sistēmas lietotāja saglabātajai informācijai, kas atrodas uz Informācijas sistēmas lietotāja datoriem vai serveriem, tikai pildot amata pienākumus vai pildot direktora rīkojumus.

35. Darbiniekiem ir aizliegts sūtīt tā sauktās “ķēdes vēstules” (t.sk. mēstules, reklāmas, aģitācijas un tml.) – elektroniskus ziņojumus ar lūgumu pārsūtīt tos citiem adresātiem, kā arī ir aizliegts atvērt un darbināt no Interneta tīkla saņemtus aizdomīgus failus. Informācijas sistēmas lietotājam ir jāatceras, ka Interneta tīkls nav droša datu pārraides platforma un nosūtītāja identifikāciju var viegli viltot. Ja par failu rodas šaubas, Informācijas sistēmas lietotājam ir nepieciešams sazināties ar nosūtītāju un noskaidrot, vai šāds dokuments ir ticis nosūtīts.

36. Darbinieki ārpus Iestādes nedrīkst sūtīt e-pastu vairākiem adresātiem vienlaicīgi, atklājot visu saņēmēju e-pasta adreses, it īpaši, ja tajās ir iekļauts personas vārds un uzvārds. Ja sūta e-pastu vairākiem adresātiem vienlaicīgi, tad izmantot diskrēto kopiju lauku (Bcc), nevis (Cc) lauku, kas saņēmējiem paslēpj visas (Bcc) laukā norādītās e-pasta adreses.

V. Informācijas sistēmas lietotāja pieejas paroles uzbūve un lietošana

37. Iestādes informācijas resursu aizsardzība tiek nodrošināta ar datora paroli datortīkla (domēna) līmenī, kam ir jāatbilst vismaz sekojošām prasībām:

37.1. minimālam paroles garumam ir jābūt vismaz 9 simboliem;

37.2. maksimālais paroles maiņas periods nedrīkst būt ilgāks par 90 dienām, taču paroli aizliegts pašrocīgi mainīt biežāk nekā divas reizes 24 stundu laikā;

37.3. paroles uzbūvei jābūt komplicētai, izmantojot vismaz vienu lielo latīņu alfabēta burtu, mazo latīņu alfabēta burtu, ciparu un īpašo rakstzīmju kombināciju (kā piemēram, !@#\$\$%^*()_+);

37.4. izveidojot paroli, tā nedrīkst sakrist ar nevienu no 5 iepriekšējām parolēm.

38. Informācijas sistēmas lietotājs nedrīkst izpaust savu paroli jebkurām citām trešajām personām vai citiem lietotājiem, izņemot atsevišķos gadījumos savas prombūtnes laikā, ja atļauju ir devis Iestādes direktors.

39. Informācijas sistēmas lietotājs nedrīkst savu paroli pierakstīt uz papīra, ja šo dokumentu neglabā seifā vai citā vietā ar ierobežotu citu personu piekļuvi.
40. Ja Informācijas sistēmas lietotājam rodas aizdomas, ka viņa paroli ir uzzinājusi jebkura cita persona, Informācijas sistēmas lietotājam ir pienākums pēc iespējas īsākā laikā šo paroli nomainīt patstāvīgi vai lūgt IT speciālistu to izdarīt savā vietā.
41. Informācijas sistēmas lietotājs ir atbildīgs par informācijas aizsardzību un tā pienākums ir nodrošināt, ka datoriem Informācijas sistēmas lietotāja prombūtnes laikā ir ieslēgts ar paroli aizsargāts ekrānsaudzētājs vai noslēgta datora darbvirsma ar Windows + L taustiņu kombināciju.
42. Dienas beigās, beidzot darbu pie datora, tas jāizslēdz, izmantojot procedūru: Start => Shut Down (vai Instal updates and shut down) => Ok.

Pielikumā:

1. Jelgavas Mūzikas vidusskolas Informācijas sistēmu tiesību pieprasījums uz 1 lpp.

1. PIELIKUMS
Jelgavas Mūzikas vidusskolas
Informācijas sistēmas lietošanas noteikumi

INFORMĀCIJAS RESURSU LIETOTĀJA REĢISTRĀCIJAS ANKETA

Piešķirt pieeju sekojošiem informācijas resursiem. vajadzīgos atzīmēt ar

- E-pasts
- Grāmatvedības uzskaites sistēma (Horizon)
- VIIS
- _____
- _____
- _____
- _____
- _____

(Datums, paraksts)