LATVIJAS REPUBLIKA
KULTŪRAS MINISTRIJA
LIEPĀJAS DIZAINA UN MĀKSLAS VIDUSSKOLA
Reģ. Nr.3031301254
Alejas ielā 18, Liepājā, LV-3401
Tālruņi: 634 23192, 634 22923, fakss 634 23192, e-pasts: info@ldmv.edu.lv

NOTEIKUMI
Liepājā

PERSONU DATU AIZSARDZĪBAS UN APSTRĀDES KĀRTĪBA

21. 05.2014. Nr.1-8./2.-20

Izdoti saskaņā ar
„Fizisko personu datu aizsardzības likumu”,
Ministru kabineta 2001.gada 30.janvāra noteikumiem Nr.40
„Personas datu aizsardzības obligātās tehniskās un
organizatoriskās prasības” 5.punktu,
Informācijas atklātības likumu

1.Vispārīgie noteikumi un termini

1. Šie noteikumi nosaka kārtību/procedūru, kādā Liepājas Dizaina un mākslas vidusskolā (turpmāk- Skolā) tiek aizsargātas datu apstrādes sistēmas, personas dati, datu pārraide iekšējā tīklā un novērsta nesankcionēta iekļūšana pašvaldības datortīklā no ārienes.
2. Noteikumu mērķis ir nodrošināt datu aizsardzību Liepājas Dizaina un mākslas vidusskolā atbilstoši normatīvajos aktos noteiktajām prasībām.
3. Personas datu apstrāde tiek veikta Skolas telpās.
4. Noteikumi ir saistoši visiem lietotājiem. Noteikumi ir attiecināmi uz visiem personas datiem, kas attiecas uz identificētu vai identificējamu fizisko personu.
5. Par informācijas drošību pašvaldībā kopumā atbild Skolas direktors.
Izmantotie termini
6. Datu subjekts – fiziskā persona, kuru var tieši vai netieši identificēt.
7. Datu subjekta piekrišana – datu subjekta brīvi, nepārprotami izteikts gribas apliecinājums, ar kuru datu subjekts atļauj apstrādāt savus personas datus atbilstoši pārziņa sniegtajai informācijai.
8. Personas dati – jebkāda informācija, kas attiecas uz identificētu vai identificējamu fizisko personu.
9. Personas datu apstrāde – jebkuras ar personas datiem veiktas darbības, ieskaitot datu vākšanu, reģistrēšanu, ievadīšanu, glabāšanu, sakārtošanu, pārveidošanu, izmantošanu, nodošanu, pārraidīšanu, izpaušanu, bloķēšanu vai dzēšanu.
10. Personas datu apstrādes sistēma – jebkurā formā fiksēta strukturēta personas datu kopa, kas ir pieejama, ievērojot attiecīgus personas identifikācijas kritērijus.

11. Pārzinis – fiziska vai juridiska persona, kura nosaka personas datu apstrādes mērķus un apstrādes līdzekļus.
12. Drošības prasības – prasības, kas jāievēro, lai nodrošinātu datorsistēmu un datu aizsardzību pret bojāšanu, zaudēšanu vai nesankcionētu izmantošanu.
13. Informācijas resursi – pieejamā programmatūra un aparatūra, kas paredzēta informācijas apstrādei vai vadībai.
14. Datortīkla administrators – darbinieks, kura pārvaldījumā nodoti informācijas resursi.
15. Lietotājs – darbinieks, kam dotas tiesības lietot datorsistēmas un datus.
16. Serveris – datu uzturēšanas aparatūra, kas nodrošina datu bāžu uzturēšanu.

2.Informācijas klasifikācija

17. Informācijas klasifikācijas līmeņi:
17.1. slepena – augstākais līmenis. Šīs informācijas izpaušana vai nozagšana var radīt ievērojamus vai ilgstošus zaudējumus un nopietni kaitēt Pašvaldības labajai slavai. Strādājot ar šo informāciju ir jāievēro vislielāko piesardzību un šo informāciju drīkst izpaust tikai ārkārtējas nepieciešamības gadījumos.
17.2 ierobežotas piekļuves – ikdienas darbā paredzētā informācija, kas paredzēta tikai noteiktam darbinieku lokam. Šīs informācijas izpaušana vai nozagšana var radīt Skolai iekšējas vai ārējas neērtības. Piekļuvi šai informācijai piešķir tikai pilnvarotiem darbiniekiem.
17.3. neklasificēta – informācija, kas jau sabiedrībai zināma, ko brīvi izplata vai kas pieejama visiem Skolas darbiniekiem un citām trešajām personām. Šīs informācijas izpaušana vai nozagšana neietekmē Skolas darbu.
17.4 Dati, kas tiek izmantoti Personas datu apstrādē, ir klasificējami kā ierobežotas piekļuves informācija, kurai ir tiesības piekļūt un veikt to apstrādi tikai pilnvarotiem darbiniekiem.

3. Lietotāju tiesību piešķiršana un administrēšana

18. Pašvaldības institūcijas, fiziskās un juridiskās personas, kas veic vai vēlas uzsākt personas datu apstrādi, reģistrē to šajā likumā noteiktajā kārtībā.
19. Datu valsts inspekcija lēmumu par personas datu aizsardzības speciālista reģistrāciju pieņem 15 dienu laikā pēc visas šā panta piektajā daļā minētās informācijas iesniegšanas Datu valsts inspekcijai.
20. Datu valsts inspekcija, kontrolē un uzrauga pārziņa veiktās personas datu apstrādes atbilstību likuma prasībām.
21. Personas datu aizsardzības speciālista pienākums ir saglabāt un bez tiesiska pamata neizpaust personas datus arī pēc darba tiesisko vai dienesta attiecību izbeigšanas.
22. Reģistrējot personas datu apstrādi, Datu valsts inspekcija izsniedz pārzinim vai viņa pilnvarotai personai personas datu apstrādes reģistrācijas apliecību.
23 Ja mainās pārzinis vai pārziņa darbība tiek izbeigta, viņš iesniedz Datu valsts inspekcijai iesniegumu par personas datu apstrādes izslēgšanu no personas datu apstrādes reģistra.
24. Skola reizi divos gados iesniedz Datu valsts inspekcijai audita atzinumu par personas datu apstrādi, ietverot tajā arī riska analīzi, un pārskatu par informācijas drošības jomā veiktajiem pasākumiem. Prasības audita atzinumam nosaka Ministru kabinets.

4. Lietotāju pienākumi

25. Lietotājs ir atbildīgs par datorsistēmu izmantošanu tikai darba vajadzībām un atbilstoši ekspluatācijas noteikumiem.
26 Lietotājs ir disciplināri, administratīvi, civiltiesiski un krimināltiesiski atbildīgs par

visām darbībām, kas veiktas datorsistēmā (informācijas ievadīšana, izmantošana, nosūtīšana, apskate un citas darbības) un par sekām, kas var rasties ikvienas datorsistēmā veiktas nesankcionētas darbības vai bezdarbības dēļ, izmantojot viņa lietotājvārdu vai paroli.
27. Lietotājs drīkst reģistrēties tikai ar savu individuālo lietotājvārdu un paroli.
28. Datu apstrādei lieto tikai konkrētajam mērķim paredzēto programmatūru vai informācijas sistēmu. Lietotājs, pārtraucot darbu ar datoru uz ilgāku laiku, aizver lietoto programmatūru vai informācijas sistēmu.
29. Lietotājiem aizliegts:
-izplatīt programmatūru un informāciju par licencēm;
-izmantot no interneta vai cita datortīkla iegūtu programmatūru;
-izplatīt dienesta informāciju ārpus iestādes;
-veikt nesankcionētas darbības ar iestādes datortīklu un datortīkla tehniku;
- veikt nesankcionētas darbības interneta tīklā, iekštīklā vai lokālajā datortīklā pret citiem šo tīklu lietotājiem;
-pieļaut trešo personu piekļūšanu interneta tīkla, iekštīkla, lokālā tīkla resursiem un programmatūrai vai informācijas sistēmām no sava un citu lietotāju datoriem.
30. Datorsistēmā drīkst atrasties tikai licencēta programmatūra. Datorsistēmā kategoriski aizliegts uzstādīt un glabāt nelicencētas programmatūras un veikt ar tām datu apstrādi
31. Programmatūru, kuras tiek izmantotas Skolas administrācijā, licences glabājas pie datortīkla administratora. Lietotājam ir kategoriski aizliegts patvaļīgi uzstādīt, glabāt vai lietot kādu citu nelicencētu programmatūru.
32. Lietotājiem tiek nodrošināta pieeja datorsistēmai. Katram lietotājam ir piešķirts unikāls lietotājvārds un parole.
33. Lietotājs drīkst piekļūt un lietot datorsistēmu, izmantojot tikai to datoru, kas ir nodots viņam lietošanā ar datortehnikas un programmatūru pieņemšanas-nodošanas aktu atbilstoši iestādes datortehnikas lietošanas noteikumiem.
34. Lietotājam kategoriski aizliegts izmantot interneta pakalpojumus, kas ļauj vienam lietotājam sazināties ar citiem lietotājiem reālā laikā jeb sarunu kanālos (piemēram, Skype) failu apmaiņas klientus (perr to perr vai torrent tīklos), kā arī lietot interneta radio vai veikt citas darbības, kas nevajadzīgi noslogo datu pārraides kanālu.
35. Lietotāja pienākums ir lietot antivīrusa programmatūru aizdomīgo failu pārbaudei. Aizliegts atslēgt antivīrusu programmatūru.
36. Aizliegts pieslēgt klēpjdatoru tīklam un lietot bez antivīrusa programmatūras.
37. Lietotājs ir atbildīgs par antivīrusu programmatūras bāzes atjaunošanu, pieslēdzot klēpjdatoru datortīklam, kad vien tas ir iespējams.
38. Lietojot datortehniku, jāievēro sekojoši ekspluatācijas noteikumi:
-pret datortehniku jāizturas saudzīgi;
-jāizvairās no iespējamas datortehnikas pārkaršanas un jāpārliecinās, ka nav aizsegti datortehnikas ventilatori;
-datortehnikai jāatrodas uz līdzenām un stabilām darba virsmām;
-uz datortehnikas nedrīkst novietot nepiederošus priekšmetus (dokumentu mapes, puķupodus, u.c.);
-nedrīkst pieskarties vai spiest uz monitora ekrāna vai displeja;
-patvaļīgi veikt datortehnikas labošanas darbus;
-nedrīkst plēst nost uzlīmes ar programmatūras autentifikācijas numuru un inventāra numurus vai aplīmēt datortehniku ar uzlīmēm;
-nedrīkst pakļaut datortehniku tiešai saules staru iedarbībai, lietus, ķimikāliju vai citu šķidrumu iedarbībai;
-gadījumos, kad datortehnikā iekļuvis šķidrums, atvienot to no elektrotīkla un par notikušo ziņot datortīkla administratoram;
-aizliegts novietot sildītāju vai citu karstuma vai uguns avotu datortehnikas tuvumā;

-aizliegts datortehnikai paredzētajās (speciāli apzīmētajās, norādītajās) elektrības rozetēs pieslēgt citas elektroiekārtas;
-nedrīkst pakļaut datortehniku stipru mehānisku spēku ietekmei;
-klēpjdatori jāpārnēsā tikai atbilstošā somā;
-darba dienas beigās, beidzot darbu, datortehnika jāizslēdz.
39. Lietotājam jāievēro un jāizpilda visi drošības noteikumi un procedūras, datortīkla administratora izvirzītie papildu drošības noteikumi un procedūras.
40. Lietotājs ir atbildīgs par visām darbībām, kas veiktas, izmantojot viņam piešķirtās tiesības informācijas resursu lietošanai. Ja lietotājs konstatē, ka viņa tiesības izmantojis kāds cits, par to nekavējoties jāziņo datortīkla administratoram.
41. Lietotājs pilnībā atbild par viņa rīcībā esošās informācijas (neattiecas uz datubāzēm, kas glabājas uz atsevišķa servera, centrālās datu bāzes) drošību, rezerves kopiju drošību un rezerves kopiju savlaicīgu sagatavošanu. Skolas informatīvās sistēmas centrālās datu bāzes rezerves kopiju nodrošināšanu un veidošana veic šīs datu bāzes, servera uzturētājs.
42. Lietotājs drīkst izpaust savā rīcībā esošo iestādes informāciju vienīgi ar tās īpašnieka rakstisku atļauju. Lietotāju pienākums ir pēc datu subjekta pieprasījuma, sniegt tam visu informāciju, kas savākta par atbilstošo datu subjektu.
43. Informāciju, kas nepieciešama pieejai informācijas resursam (parole, identifikators, u.c.) ir aizliegts izpaust, un lietotājs ir personīgi atbildīgs par tās konfidencialitāti arī pēc darba tiesisko attiecību izbeigšanas.
44. Lietotājiem ir tiesības pieprasīt lietotāju atbalstu gadījumā, ja datoram vai tā programmatūrai ir radušies traucējumi vai arī lietotājam ir pietiekams uzskats par iespējamo draudu (apdraudējumu) esamību.
45. Lietotāju pienākums ir iepazīties ar Noteikumiem un ievērot tos ikdienas darbā.
46 Pieņemot darbā jaunus darbiniekus Skolas vadītāja pienākums ir iepazīstināt darbiniekus ar vispārīgiem Skolas drošības noteikumiem. Nepieciešamības gadījumā darbinieki jānodrošina ar attiecīgu apmācību.

5. Drošības noteikumi

47. Mainīt, dzēst vai pievienot informācijas sistēmā atrodošos datus drīkst tikai un vienīgi pēc iepazīšanās ar Skolas informācijas sistēmas iekšējiem drošības noteikumiem – kad piešķirta oficiāla pieeja informācijas sistēmai un nepieciešamās tiesības, kuru ievērošanu apliecina ar parakstu (skat. pielikumu Nr.1).
48. Informāciju ārpus Skolas atļauts izpaust tikai ar informācijas īpašnieka rakstisku atļauju.
49. Dzēst vai kā citādi iznīcināt Skolas informāciju atļauts tikai ar īpašnieka atļauju.
50. Nelicencētas programmatūras uzstādīšana un lietošana ir aizliegta.
51. Jebkuru programmatūru, kas neietilpst standarta lietotāja darba stacijas konfigurācijā vai kuru nav uzstādījis Datortīkla administrators, lietotājs drīkst uzstādīt un lietot tikai ar Datortīkla administratora atļauju.
52. Licencētas programmatūras kopēšana (tai skaitā rezerves kopēšana) atļauta vienīgi tādos gadījumos, ja to atļauj attiecīgās programmatūras licencēšanas noteikumi.
53 Jebkura ienākošā elektroniskā informācija pirms lietošanas obligāti jāpārbauda ar pretvīrusu programmatūru, ja tas netiek nodrošināts automātiski.
54. Lietotājam aizliegts deinstalēt vai deaktivizēt instalētās pretvīrusu programmas.
55. Gadījumā, ja programmas nefunkcionē tā, kā paredzēts, vai arī tās darbība šķiet aizdomīga, par to nekavējoties jāziņo Datortīkla administratoram. Ja ir aizdomas par drošības pārkāpumu vai datorvīrusu, jārīkojas šādi:
- Jāiegaumē aizdomīgās pazīmes un paziņojumi, kas parādās uz ekrāna;
- Dators jāatvieno no tīkla un jāpārtrauc tā lietošana;
- Aizliegts patstāvīgi mēģināt deaktivizēt un deinstalēt aizdomīgo programmatūru;

• Disketes vai citus datu nesējus, kas atradušās attiecīgajā datorā, līdz apstākļu tālākai noskaidrošanai aizliegts izmantot citos datoros;
• Par notikušo nekavējoties jāziņo datortīkla administratoram.
56. Datortīkla administratoram pienākums ir operatīvi reaģēt, lai lietotājs ārkārtas gadījumos varētu nekavējoties turpināt darbu.
57. Aizliegts iznest vai izsūtīt Skolai piederošu programmatūru vai dokumentāciju ārpus Skolas telpām bez datortīkla administratora atļaujas.
58. Beidzot darbu ar datu bāzi, tā obligāti jāatslēdz.
59. Bez datortīkla administratora atļaujas aizliegts pieslēgt datortīklam vai atslēgt no tā jebkādas iekārtas, izņemot Skolai piederošos portatīvos datorus.
Jebkādu ierīču pieslēgšana datoram vai atslēgšana no tā, kā arī datortehnikas konfigurācijas maiņa (ieskaitot BIOS parametrus) jāsaskaņo ar Datortīkla administratoru.
60. Datortīkla administrators nodrošina rezerves kopēšanu un kopiju uzglabāšanu informācijai, kas atrodas uz failu vai datu serveriem. Uz darba stacijas esošās informācijas rezerves kopēšana netiek nodrošināta.
61. Aizliegts piešķirt citiem lietotājiem attālinātu pieeju savas darba stacijas vai portatīvā datora resursiem.
62. Darbu beidzot (darba dienas beigās), lietotājam jāaizver visi lietojumi un jāatslēdzas no lokālā datortīkla, izpildot datora slēgšanas (shut down) funkciju.
63. Ja no darbinieka datora pēc darba laika beigām tiek darbināti ilglaicīgi procesi, tad par to jāinformē Datortīkla administrators.
64. Ja notiek informācijas resursu bojāšanās, tad tie tiek atjaunoti šādā kārtībā (prioritārie ir pirmie uzskaitījumi:
• serveris;
• darba stacijas;
• citi informācijas resursi.

6. Interneta lietošana

65. Internet izmantošana atļauta vienīgi darba pienākumu veikšanai (tai skaitā pašizglītībai darba jautājumos).
66. Visa no Internet tīkla saņemtā informācija jāpārbauda ar pretvīrusu programmām (gan programmatūra, gan arī datu faili), ja tas netiek nodrošināts automātiski.
67. Gadījumā, ja rodas aizdomas par drošības pārkāpumiem, kas varētu būt saistīti ar Internet lietošanu, nekavējoties jāiziet no Internet un no visām tobrīd lietotām informācijas sistēmām un par notikušo jāinformē Datortīkla administrators.
68. Aizliegts vienlaicīgi lietot Internetu un datu bāzes.
69. Lietojot iestādes interneta pieslēgumu, lietotājam jāņem vērā, ka datortehnikas administratoram ir tiesības:
• pilnībā vai daļēji ierobežot piekļuvi interneta tīmekļa vietnēm darba un ārpus darba laika, kas saistītas ar izklaidi un servisiem, kuri nav nepieciešami darba pienākumu izpildei;
• aizliegt piekļuvi interneta tīmekļa vietnēm, kas saistītas ar vardarbības propagandēšanu, seksuālu materiālu publicēšanu, tērzēšanas servisiem, alkohola un narkotiku popularizēšanu, azartspēlēm u.c.
• vākt un uzkrāt statistisko informāciju par interneta datu plūsmu un tīkla noslodzi (ieskaitot informāciju par konkrētiem datoriem), lai analizētu tīkla noslodzi.

7. Elektroniskā pasta lietošana

70. Elektronisko pastu atļauts izmantot vienīgi darba vajadzībām.

71. Aizliegts sūtīt „ķēdes vēstules”- elektroniskā pasta vēstules, parasti ar izklaidējošu saturu un lūgumu pārsūtīt tās citiem adresātiem. 6
72. Aizliegts pārsūtīt informāciju, kas pārkāpj Latvijā spēkā esošo likumu par autortiesībām un citus normatīvos aktus.
73. Aizliegts atvērt un darbināt no nezināmiem avotiem saņemtus failus, par kuru saturu nav pārliecības. Ja par failu saturu rodas šaubas, vēlams pārvaicāt nosūtītājam, vai šāda satura dokuments ir ticis izsūtīts.
74. Lietotājiem, izmantojot e-pastu, aizliegts:
• izplatīt pornogrāfiska un vardarbību propagandējoša satura materiālus;
• izplatīt Skolas iekšējā tīklā masveida ziņojumus (informāciju par kādiem pasākumiem, notikumiem vai citu informāciju, ja tā neattiecas uz konkrētu adresātu), kas varētu traucēt citu lietotāju darbu un lieki noslogot Skolas datortīklu;
• sūtīt ziņojumus, par kuru nokļūšanu līdz adresātam sūtītājam ir šaubas;
• sūtīt vienā elektroniskā pasta sūtījumā informāciju, kuras apjoms ir lielāks par 10 MB, kā arī vairākus e-pasta sūtījumus ar maksimāli pieļaujamo apjomu vienam adresātam;
• uzstādīt citas, atšķirīgu no Microsoft Outlook, Outlook Express e-pasta klienta programmatūru.

8. Paroļu lietošana

75. Informācijas sistēmas aizsardzība tiek nodrošināta ar datora paroli.
76. Nav pieļaujama lietotāja paroles izpaušana citai personai. Gadījumos, kad ir nepieciešama darbinieka aizvietošana, iestādes vadītājs pieprasa novada administrācijas datorspeciālistam nepieciešamā lietotāja konta izveidi vai esošā lietotāja konta tiesību izmaiņu uz noteiktu laiku.
77. Parole ir nekavējoties jānomaina, ja to ir uzzinājis kāds cits vai ir aizdomas, ka to ir uzzinājis kāds cits. Paroli nav atļauts sūtīt pa elektronisko pastu vai kā citādi darīt zināmu.
78. Lietotāju paroles tiek veidotas, ņemot vērā šādus kritērijus:
• parole jāsastāda tā, lai to var atcerēties nepierakstot;
• parolei jāsatur ne mazāk kā astoņi simboli (lielie, mazie burti, cipari un simboli);
parole nedrīkst saturēt:
• lietotājvārdu vai daļu no tā;
• iepriekš lietotās paroles;
• lietotāja radinieku vārdus vai uzvārdus;
• savu mājdzīvnieku vārdus;
• lietotāja vai viņa kolēģu telefona numurus, personas kodus;
• simbolu virkni no blakus esošiem klaviatūras taustiņiem;
• burtus ar garumzīmēm vai mīkstinājuma zīmēm;
• parolei jābūt ne īsākai par 8 zīmēm, no kurām vismaz divām ir jābūt ciparіem vai speciāliem simboliem.
79. Savas paroles – kā pašreizējās, tā arī agrāk lietotās – aizliegts izpaust citām personām.
80. Aizliegts mēģināt izzināt svešas paroles.
81. Gadījumā, ja ir aizdomas, ka paroli varētu būt uzzinājušas citas personas, tā nekavējoties jāmaina.
82. Aizliegts izmantot automatizētas pieslēgšanās programmatūru.
83. Aizliegts piekļūt informācijas resursiem ar svešu identifikatoru un paroli.
84. Lietotājs ir atbildīgs par viņa lietošanā esošo paroļu drošību. Paroles jācenšas iegaumēt, bet gadījumos, kad tas nav iespējams (piemēram, ja tā ir parole, kas paredzēta ārkārtas gadījumiem), tās jāuzglabā aizzīmogotās aploksnēs.
85. Lietotājs ir atbildīgs par visām darbībām, kas veiktas, lietojot viņa identifikatoru.

86. Gadījumā, ja ir aizdomas, ka identifikatoru un paroli izmantojusi (vai mēģinājusi izmantot) cita persona, par to nekavējoši jāinformē Datortīkla administrators.
87. Datortīkla administrators paroli vai citu identifikatoru anulē nekavējoties pēc Lietotāja saņemtā ziņojuma par paroles vai identifikatora nozaudēšanu vai nokļūšanu trešās personas rīcībā. Ja paroles vai identifikatora maiņa Lietotāja rīcības dēļ notiek trīs reizes gada laikā Datortīkla administrators par to raksta ziņojumu izpilddirektoram, kurš izlemj par Lietotāja sodīšanu vai pieejas tiesību anulēšanu.
88. Izbeidzoties darba attiecībām ar darbinieku, kuram bija pieejas tiesības informācijas resursiem un klasificētai informācijai, vienlaikus tiek anulētas paroles un identifikatori, kas nodrošināja piekļuvi.

9. Failu un katalogu nosaukumu veidošana

89. Lietotājam veidojot failu vai kataloga nosaukumus jāizmanto latīņu alfabēta burtus bez garumzīmēm un mīkstinājuma zīmēm (a; b; c; utt.), ciparus (1;2;3; utt.) pasvītrojuma zīmi _.
90. Failu un katalogu nosaukumos nedrīkst izmantot simbolus f ? : *; <; >; /; \: +: i:): !: atstarpe, komats, punkts.
91. Failu un katalogu nosaukumos nedrīkst izmantot perifērijas ierīču un portu apzīmējumus (PRN; LPT1; LPT2 utt.; COMsimbolus; COM2 utt.; CON; NUL; AUX). Lai nosaukumos atdalītu vārdus var izmantot lielos un mazos burtus (piem.: AkcijuSabiedriba) vai pasvītrojuma zīmi (Akciju_sabiedriba).

VIII. Datoru minimālās prasības

92. Ikvienam datoram jābūt aprīkotam ar minimālo licencētu programmnodrošinājumu un jāatbilst minimālajām resursu prasībām
93. Minimālais licencētais programmnodrošinājums sastāv no:
• Windows tipa vides, kura nodrošina teksta un grafisko redaktoru darbību un izdrukāšanu;
• Teksta redaktora;
• Elektroniskais tabulators (piemēram Microsoft Excel);
• Interneta pārlūkprogrammas;
• Elektroniskā pasta programmas;
• Pretvīrusu programmas.
94. Datoram jābūt nokomplektētam ar monitoru, sistēmas bloku, klaviatūru, peli, pieejamu drukas ierīci, nepārtrauktās barošanas iekārtu.
95. Kabinetā nedrīkst vienlaicīgi darboties vairāk kā divas darbstacijas un portatīvais dators.

IX. Resursu fiziskā aizsardzība

96. Visiem datoriem jāatrodas slēdzamās telpās.
97. Tīkla vadiem, kas savieno darbstacijas jābūt ievietotiem slēgtos penāļos, tā lai trešās personas nevarētu tiem brīvi piekļūt.
98. Serveris atrodas atsevišķā, servera uzturēšanai tehniskām prasībām atbilstošā telpā. Serveris ir jānodrošina ar ierīci, kas nodrošina nepārtrauktu elektrības padevi.
99. Datu nesēji, tai skaitā arī darbstacijas tiek iznīcinātas pēc to morālās un fiziskās nolietošanās.

10. Pārejas noteikumi

100. Lietotājs savas kvalifikācijas paaugstināšanai ārpus darba laika var izmantot datoru un sistēmas pakalpojumus personiskām vajadzībām.
101. Uz servera atrodošā programmnodrošinājuma rezerves kopijas tiek sagatavotas pēc vajadzības, bet ne retāk kā reizi mēnesī.
102. Informācijas resursu rezerves kopijas tiek uzglabātas uz CD-R vai CD-RW tipa informācijas nesējiem. Informācijas resursu rezerves kopijas tiek uzglabātas no servera atsevišķā telpā.

11. Atbildība

103. Par šajos noteikumos noteikto normu neievērošanu Lietotājs vai jebkurš Skolas darbinieks var tikt sodīts atbilstoši darba likumdošanā noteiktajā kārtībā.
104. Par šo noteikumu pārkāpšanu var anulēt pieejas tiesības informācijas resursiem. Ja anulētās pieejas tiesības ir nepieciešamas tiešo darba pienākumu veikšanai, tad tiek izskatīts jautājums par darbinieka atbilstību ieņemamajam amatam.
105. Skolas darbiniekiem atkarībā no pārkāpuma rakstura un sekām var tikt piemēroti arī citi atbildības veidi.

12. Rīcība problēmu gadījumā

106. Par visām avārijas situācijām (t.sk. ugunsgrēku, plūdiem, nelaimes gadījumiem utt.) lietotājiem ir nekavējoties jāpaziņo iestādes vadītājam vai tā pilnvarotai personai.

Direktore S. Rubeze