



# **KOHTLA-JÄRVE JÄRVE KOOLI INFOSÜSTEEMI KASUTAMISE KORD**

Kinnitatud 09.04.2020 direktori käskkirjaga nr 1.1-3/97

Kohtla-Järve  
2020

## SISUKORD

§ 1. Eesmärk ja reguleerimisala .....	3
§ 2. Pääsuõiguse haldamine .....	3
§ 3. Kasutajakonto loomine, haldamine ja kustutamine.....	3
§ 5. Kasutajakonto omaniku kohustused .....	5
§ 6. Kasutaja personaalsete andmete väljastamine .....	6
§ 7. Paroolinõuded .....	6
§ 8. Failihalduse teenus .....	7
§ 9. E-posti teenus .....	7
§ 10. Interneti kasutamine .....	8
§ 11. Andmekandjate kasutamine .....	9
§ 12. Arvutite kasutamine .....	9
§ 13. Nutiseadmete kasutamine .....	10
§ 14. Wifi kasutamine .....	11
§ 16. Kasutajatoe teenus .....	12

## § 1. EESMÄRK JA REGULEERIMISALA

(1) Järve Kooli infosüsteemi (edaspidi *infosüsteem*) kasutamise korra eesmärk on sätestada infovarade sh pääsuõiguste, arvutivõrgu, andmekogude ja IT-vahendite kasutamise reeglid.

(2) Korda rakendatakse Kohtla-Järve Järve Kooli (edaspidi haridusasutus) töötajate, õpilaste ja väliste kasutajate suhtes (edaspidi kõik koos ka *kasutaja*).

## § 2. PÄÄSUÕIGUSE HALDAMINE

(1) Pääsuõiguse andmisel lähtutakse kasutajate töö- või õppealase vajaduse ja minimaalsete õiguste põhimõttest. Installeerimise õigusi omavad ainult domeeni administraatorid.

(2) Pääsuõiguse andmisel asutuse välisele kasutajale (edaspidi *väline kasutaja*) lähtutakse § 3 lõikes 11 toodud nõuetest.

(3) Igal infosüsteemi kasutajal on autentimiseks personaalne kasutajanimi ja parool või kiipkaart, mida ei tohi edastada teistele isikutele.

(4) Töötajale saab infosüsteemi ja andmekogude pääsuõigusi taotleda vaid vahetu juht. Õiguste taotleja peab veenduma, et õiguste saaja on tutvunud vajalike juhendite ja kordadega (sh infosüsteemi kasutuse korruga). Töölt lahkudes töötaja saab ringkäigu lehe, mille allkirjastab ka infojuht, kui kõik IT- vahendid on tagastatud.

(5) Andmekogude pääsuõigused annab andmekogude vastutav kasutaja, kes peab arvestust pääsuõiguste väljastamise kohta.

(6) Õpilastele saavad pääsuõigusi taotleda klassijuhataja või õppejuht.

## § 3. KASUTAJAKONTO LOOMINE, HALDAMINE JA KUSTUTAMINE

(1) Arvutivõrgu (domeeni) kasutajakonto ja personaalne e-posti aadress luuakse töötajale pärast tööle võtmist ja õpilasele pärast haridusasutuse nimekirja arvamist. Konto loob haridusasutuse vastavate õigustega töötaja või IT infojuht.

- (2) Arvutivõrgu kasutajakonto annab õiguse kasutada personaalset ja jagatud võrguressurssi ning e-posti süsteemi vastavalt töö- või õppealasele vajadusele.
- (3) Esmakordsel sisselogimisel peab kasutaja kasutajakonto parooli koheselt ära muutma ainult enda teada olevaks parooliks. Alklasside õpilaste parooli võib hallata klassijuhataja.
- (4) Lepinguliste ülesannete täitmiseks lühikeseks ajaperioodiks (praktika, projektipõhine töö jne) tehakse isikule ajutine kasutajakonto, millele on määratud tähtaeg, mis ei tohi olla pikem kui lepingu tähtaeg.
- (5) Töösuhte lõppemise kuupäev on ringkäigulehel kirjas, kõik, kes allkirjastavad, teavad töötaja lahkumisest ja tema volituste lõppemisest koolis. Koolis on eraldi ringkäigulehed õpetajale (ka infojuhi allkiri) ja töötajale (pole vaja infojuhi allkirja).
- (6) Õpilase või töötaja nimekirjast välja arvamisel infosüsteemi pääsuõigus lukustatakse, konto ja sellega seotud andmed kustutatakse asutuse vastavate õigustega töötaja või IT toe poolt 3 kuu jooksul.
- (7) Töösuhte peatumisel pikemaks kui 60 päeva töötaja kasutajakonto ja juurdepääsuõigused infosüsteemile lukustatakse asutuse juhi korraldusel, mis edastatakse e-posti teel IT toele.
- (8) Töötaja peab enne töösuhte lõppemist kustutama oma postkastist, võrgukettalt ja arvuti andmekandjalt (s. h nutiseadme mälust) mittetöölalased ning ebaolulise sisuga e-kirjad ja failid.
- (9) Töösuhte lõppemisel pääsuõigused ja personaalne postkast suletakse ning saabuvat e-posti edasi ei suunata.
- (10) Kõik varukoopiatele salvestatud töötaja personaalses postkastis olevad kirjad ja võrgukettal olevad failid archiveeritakse.
- (11) Välistele kasutajatele antakse infosüsteemi pääsuõigused ainult tähtajaliselt kirjaliku taotluse alusel. Taotlusel peavad olema kirjas vähemalt isiku kontaktandmed, töökoht, juurdepääsu õiguste vajaduse põhjendus, millistele teenustele/ressurssidele on juurdepääsu vaja ning milliseks perioodiks. Kui pääsuõiguste vajadus lõpeb enne tähtaega, peab taotluse esitanud isik sellest koheselt IT toele kirjalikult teatama. Pääsuõigusi auditeerib asutuse juht või infoturbe eest vastutav isik.

(12) Arvutiklassis toimuvatele üritustele (olümpiaadid, nutivõistlused), milles osalevad teiste koolide õpilased, tuleb vastutaval isikul taotleda kontode loomisest infojuhi poolt vähemalt 2 päeva enne üritust. Konto loomiseks esitada osalevate õpilaste nimekiri.

#### § 4. KASUTAJAKONTO OMANIKU ÕIGUSED

Kasutajal on õigus:

- 1) omada juurdepääsu talle tööülesannete täitmiseks vajalikule teabele ja teenustele kokku lepitud tööajal;
- 2) saada mõistliku aja jooksul infot planeeritud muudatustest ja häiretest süsteemides ning arvutivõrgus;
- 3) pöörduda infotehnoloogiaalase abi saamiseks IT toe poole § 17 kirjeldatud viisil;
- 4) saada infot temaga seotud arvutivõrgu kasutamise logide, personaalsel võrgukettal ning personaalse elektronposti kasutajakontol olevate andmete kohta;
- 5) töödelda (vaadata, muuta, väljastada) konfidentsiaalset informatsiooni (teave, mis seaduse, lepingu või mõnel muul alusel kuulutatud mitteavalikuks) ainult oma otseste töö- või ametiülesannete täitmiseks. Eelpool nimetatud teavet ei tohi edastada kolmandatele isikutele juurdepääsupiirangu kehtestanud asutuse loata.

#### § 5. KASUTAJAKONTO OMANIKU KOHUSTUSED

Kasutaja on kohustatud:

- 1) kasutama võrguressursse optimaalselt ning mitte koormama arvutivõrku mittetöölalaste tegevustega;
- 2) regulaarselt korrastama personaalset e-posti ja failiserveris asuvaid andmeid, kustutades ebaolulise sisuga kirjad ja failid. Pidama kinni infosüsteemis kehtestatud mahupiirangutest;
- 3) riist- ja tarkvara lisamiseks, ümberpaigutamiseks, häälestamiseks ja eemaldamiseks pöörduma IT-toe poole itabi@jarve.edu.ee;
- 4) mitte ühendama asutuse sisevõrku asutusele mittekuuluvat riistvara;
- 5) arvuti juurest lahkudes välja logima enne järgmise tunni algust selle või arvuti sulgema koolipäeva lõpus;
- 6) hoidma enda teada paroolid. Kui parool on saanud teatavaks kõrvalistele isikutele või on kahtlus, et see on võinud juhtuda, on kasutaja kohustatud parooli koheselt muutma või laskma selle IT toe kaudu tühistada.

## § 6. KASUTAJA PERSONAALSETE ANDMETE VÄLJASTAMINE

(1) Paragrahvi 4 punktis 4 nimetatud andmete väljastamine või neile juurdepääsu võimaldamine toimub üksnes:

- 1) kasutajale endale;
- 2) kolmandale isikule kasutaja kirjalikul nõusolekul;
- 3) seadusega ettenähtud korras;
- 4) kasutaja suhtes algatatud distsiplinaarmenetluses või töölepingu alusel tegutseva töötaja poolt lepingu rikkumise korral vastavalt asutuse juhi poolt kehtestatud korrale (käskkirjale).
- 5) töötaja tööülesannete üleandmisel teisele töötajale

(2) käesoleva paragrahvi lõike 1 punktides 4 ja 5 nimetatud juhul edastab asutuse juht vastavasisulise info e-posti teel IT toele.

## § 7. PAROOLINÕUDED

(1) Esmaselt väljastatud parool on ühekordne (kui vastava infosüsteemi või andmekogu kasutusjuhendis ei ole märgitud teisiti) ning kasutaja kohustub selle vahetama esimesel sisselogimisel ainult temale teadaoleva parooli vastu.

(2) Parool peab koosnema suur- ja väiketähtede ning numbrite kombinatsioonist. Soovitav on lisaks kasutada kirjavahemärke. Parooli pikkus peab olema vähemalt 10 sümbolit. Parool ei tohi olla kergesti aimatav (näiteks nimed, auto numbrimärgid, sünnikuupäevad) ega sisaldama täpitähti.

(3) Maksimaalne parooli kehtivusaeg asutuse infosüsteemis on 180 päeva.

(4) Parooli vahetamisel peab infosüsteem meeles viis viimast parooli.

(5) Viiekordsel vale parooli sisestamisel konto lukustatakse. Konto avab asutuse vastavate õigustega töötaja või IT tugi.

## § 8. FAILIHALDUSE TEENUS

(1) Iga kasutaja jaoks võib vajadusel eraldada personaalse võrguketta ja mahu serveris, millele ligipääs on vaid kasutajal endal.

(2) Võrgukettal hoitakse kasutaja personaalseid töökaustu (Dokumendid, Töölaud, Pildid).

(3) Töötajale juurdepääsu andmine jagatud võrguketastele toimub ainult vahetu juhi kirjaliku taotluse alusel lähtudes tööalasest vajadusest.

(4) Õppetööks vajalikke jagatud kaustu võib luua õppejuhi kirjaliku taotluse alusel määrates kettaressursile vastutava kasutaja (omaniku).

(5) Töötaja peab hoidma tööalaseid faile failiserveri võrguketastel. Varundamine tagatakse vaid töökaustadele ja võrguketastel olevatele failidele.

(6) Kasutaja peab vältima suuremahulise info salvestamist Töölauale.

(7) Isiklikke faile tohib hoida arvuti kõvakettal kataloogis „Isiklik“ omal vastutusel ja jälgides, et tööks vajalik ketta maht oleks piisav. Isiklikke faile ei tohi hoida töökaustades.

(8) Suuremahuliste failide jagamiseks võib kasutada ainult asutuse hallatavat pilveteenust.

## § 9. E-POSTI TEENUS

(1) Kõigil on ühtne IT toe hallatav e-postisüsteem domeeninimega jarve.edu.ee

(2) E-posti süsteemi võib kasutada nii veebipõhiselt kui arvutisse paigaldatud e-posti tarkvaraga järgides infoturbenõudeid.

(3) Igal töötajal ja õpilasel on personaalne e-posti konto kujuga [eesnimi.perenimi@jarve.edu.ee](mailto:eesnimi.perenimi@jarve.edu.ee). Töötajatel on koos e-postiga võimalik kasutada kalendrite ja pilveketta teenust. Samanimeliste kasutajate korral lisatakse kasutajaga kokkuleppel perenimele number.

(4) E-posti konto võib olla ka asutusel või kindla funktsiooni täitmiseks. Igal e-posti kontol on vastutav kasutaja.

(5) Asutusesisese töö korraldamiseks võib IT tugi luua aadresside liste.

(6) E-posti kontol on mahupiirang 4 GB. Iga e-posti aadressi omanik on kohustatud jälgima, et postkastis oleks käideldavuse tagamiseks piisav mahu varu.

(7) Kasutajal on keelatud avada kahtlusi tekitava pealkirjaga, sisuga või kahtlustäratavalt aadressilt saabuvald kirju ning käivitada neis olevaid hüperlinke ja manuseid.

(8) Keelatud on asutuse e-posti aadressi kasutamine tarbijamängude mängimiseks, isiklike kommertsteadete tellimiseks, mitte tööalaste foorumite kasutamiseks ning muudeks tegevusteks, mis võivad põhjustada hulgalise kommertsteadete ja rämpsposti saatmise.

(9) Kasutaja ei tohi suunata asutuse e-posti automaatselt edasi asutusevälistele aadressidele. Käsitsi edastamisel tuleb jälgida konfidentsiaalsusnõudeid. Õpilastel e-posti automaatse suunamise võimalus puudub.

(10) Dokumentide edastamisel tuleb eelistada *pdf* vormingut.

(11) Tööalast informatsiooni võib edastada ainult asutuse e-posti süsteemi kaudu.

(12) Konfidentsiaalse info saatmisel väljapoole asutust tuleb see krüpteerida.

(13) Suuremahuliste failide saatmist e-posti manusena tuleb vältida. E-kirja maht ei tohi ületada 20MB. Suure mahuga infot võib edastada asutuse pilveteenuse kaudu lingiga.

## § 10. INTERNETI KASUTAMINE

(1) Interneti kasutamisega seotud andmed logitakse.

(2) Kasutajal on keelatud asutuse seadmesse laadida omavoliliselt (ilma IT toe loata) alla tarkvara ja tarkvarauuendusi, mängu, filme jms.



(3) Töötajal on keelatud esineda sotsiaalvõrgustikes kellegi teisenä varjates oma identiteeti.

(4) Töötajal on internetis uudiseportaalide ning elektroonilise ajakirjanduse uudiste või artiklite kommenteerimine lubatud üksnes juhul, kui ta teeb seda oma nime alt oma töövaldkonna kohta ning kooskõlastab selle eelnevalt vahetu juhiga.

## § 11. ANDMEKANDJATE KASUTAMINE

(1) Eemaldatevate andmekandjate kasutamine on kõrgendatud ohu allikas. Neid on lihtne kaotada, varastada, need võivad rikneda ja neid võidakse kasutada arvuti pahavaraga nakatamiseks.

(2) Infosüsteemis tohib kasutada vaid IT toe poolt lubatud digitaalseid andmekandjaid.

(3) Konfidentsiaalse informatsiooni salvestamine eemaldatevadele digitaalsele andmekandjale on lubatud ainult tööülesannete täitmiseks.

(4) Konfidentsiaalset informatsiooni sisaldava andmekandja kadumisest või vargusest tuleb koheselt teavitada asutuse IT tuge.

(5) Kasutusest eemaldatev digitaalsetel andmekandjatel oleva info hävitamise korraldab IT tugi.

## § 12. ARVUTITE KASUTAMINE

(1) Arvutites kasutatav tarkvara on: süsteemitarkvara, baastarkvara, standardtarkvara, lisatarkvara.

(2) Arvutil on üldjuhul üks kasutaja.

(3) Ühiskasutuses või mitme kasutaja puhul määratakse arvuti väljastamisel arvuti eest vastutav kasutaja.

(4) Töötaja peab olema tutvunud valla infoturbe poliitikaga jt infotehnoloogiat ja infoturvet reguleerivate õigusaktidega.

(5) Automaatse ekraaniluku rakendumine on kohustuslik ja seadistatakse IT toe poolt.

(6) Arvuti kasutaja kohustub:

- 1) kaugtööl järgima asutuse infosüsteemide kasutamise korda ja töökorralduse reegleid;
- 2) hoidma sülearvutit avalikes kohtades isikliku järelevalve all;
- 3) mitte laskma sülearvutit külmuda ega üle kuumeneda (otsese päikesekiirguse käes);
- 4) sülearvuti või muu IT-vahendi vargusest või kaotamisest koheselt teavitama IT tuge;
- 5) ühiskasutuses oleva arvuti puhul töö lõpetades välja logima.

(7) Konfidentsiaalse info töötlemisel kasutaja kohustub:

- 1) veenduma, et arvutiekraanil toimuv ei ole teistele isikutele nähtav;
- 2) sisestama kasutajatunnused nii, et teised isikud ei näeks mida sisestati;
- 3) mitte kasutama sülearvutit avalikus võrgus kui on kahtlus, et arvuti turvaseaded (tulemüür, viirusetõrje, VPN) ei ole töökorras ning arvestama, et väljaspool asutuse sisevõrku võidakse ühendust pealt kuulata;
- 4) viirusekahtlusega arvuti koheselt eemaldama arvutivõrgust, selle sulgema ning teatama IT toele.

(8) Asutusesisestele võrguressurssidele saab välisvõrgust ligi ainult läbi turvakanalit, mille seadistab IT tugi.

(9) Asutusesiseseks kasutamiseks või delikaatseid isikuandmeid sisaldava info töötlemiseks kasutatava sülearvuti kõvaketas peab olema krüpteeritud.

## § 13. NUTISEADMETE KASUTAMINE

(1) Tööülesannete täitmisel on lubatud kasutada ainult IT toe poolt aktsepteeritud nutiseadmeid (edaspidi *nutiseade* või *nutitelefon*).

(2) Töötajate nutiseadmed peavad olema kaitstud ekraanilukuga. Ekraanilukk peab rakenduma automaatselt. Mustrikombinatsioon ei ole piisav kaitse ja seda võib kasutada ainult koos PIN koodiga.

(3) Asutusesiseseks kasutamiseks või delikaatseid isikuandmeid sisaldavat infot ei ole lubatud nutiseadmes töödelda ega kasutada nutiseadet konfidentsiaalse info andmekandjana.

(4) Asutuse nutitelefonid ei või kasutamiseks edasi anda teistele isikutele.

(5) Nutiseadmete hankimine, hooldus ja remont käib ainult IT toe kaudu.

(6) Nutiseadme kaotamise või varastamise korral on kasutaja kohustatud koheselt teavitama IT tuge.

(7) Õppetöös kasutatavaid nutiseadmeid ei tohi siduda kasutajate isiklike kontodega, mis asuvad väliste teenusepakkujate juures.

(8) Õppetöös kasutatavate nutiseadmete sidumine väliste teenusepakkujate kontodega toimub IT toe koostööl.

#### § 14. WIFI KASUTAMINE

(1) Asutuses on koolis kolm: õpetajate võrk nimega Jarve gymnaasium (juhtkond ja õpetajad); õpilaste võrk JarveG opilane (ligipääsu saavad kooli sülearvutid ja tahvelarvutid) ja vaba võrk nimega Kylaline (ligipääs lubatud kooli külalistele).

#### § 15. KRÜPTEERIMINE

(1) Isikuandmeid või konfidentsiaalset infot sisaldavaid dokumente asutusest välja saates peavad need olema krüpteeritud. Krüpteerimiseks võib kasutada ID-kaardi lahendust kasutades personaalset või asutuse sertifikaati.

(2) ID-kaardi lahendusega krüpteeritud dokumendid tuleb säilitamiseks lahti krüpteerida.

(3) Arvutite andmekandjate krüpteerimine toimub operatsioonisüsteemi standardsete vahenditega (BitLocker) mille seadistab IT tugi.

(4) Väliste andmekandjate krüpteerimine toimub ainult IT toe poolt lubatud vahenditega mis tagavad andmekandjale piisava turvalisuse vastavalt andmete turbeastmele ja kasutuse ajahorisondile.

## § 16. KASUTAJATOE TEENUS

(1) IT-vahendite hankimist korraldab IT tugi ja nende üle peetakse arvestust IT toe hallatavas tarkvaralahenduses.

(2) IT-vahendid annab kasutajale või vastutavale kasutajale üle IT tugi ja töösuhte või vajaduse lõppemisel võtab tagasi IT tugi.

(3) Kasutaja on kohustatud esimesel võimalusel teavitama IT tuge infotehnoloogiliste teenuste kasutamist takistavatest juhtumitest, võimalikest ohtudest ja infoturbeintsidentidest. Juhtumitest teatada:

1) e-posti aadressil: [itabi@jarve.edu.ee](mailto:itabi@jarve.edu.ee)

2) telefoni teel.

(4) IT toele saabunud juhtumid registreeritakse.

(5) Juhtumi kiireks lahendamiseks on soovitatav edastada vähemalt järgmine info:

1) tõrkega seotud seadme number, nimetus, asukoht;

2) kasutaja nimi;

3) probleemi kirjeldus;

4) mida on eelnevalt tehtud juhtumi lahendamiseks (restart).

(6) Arvutihooldustöödeks või kasutaja abistamiseks võib IT tugi asutuse seadmetes kasutada kaughaldustarkvara võttes üle seadme pildi ja juhtimise ilma kasutaja aktseptita. Töötaja soovil võib tema seadmes lisada kaughaldustarkvara aktsepti päringu.