

IRDANDMEKANDJATE KASUTAMISE KORD

Ahtme Kool

1. Reguleerimisala, mõisted ja seosed teiste dokumentidega

1.1. Kord sätestab irdandmekandjate kasutamise reeglid Ahtme Koolis (edaspidi kool): põhimõtte, lubatud erandid, piirangud, vastutuse ja kontrollimeetmed.

1.2. Kord kehtib kõigile kooli töötajatele, praktikantidele ja teistele isikutele, kes kasutavad kooli arvuteid või võrku või töötlevad kooli andmeid. Õpilaste suhtes kohaldatakse punkti 2.5.

1.3. Kord ei laiene tervishoiuteenuse osutaja seadmetele ja andmetele, mida kasutab kooliõde; nõuded neile kehtestab teenuseosutaja. Kooli andmekandjaid nende seadmetega ei ühendata ja teenuseosutaja andmekandjaid kooli tööarvutitega ei ühendata.

1.4. Irdandmekandja on andmekandja, mida kasutaja saab tavapärase töö käigus arvuti või muu seadmega ühendada ja sellest lahutada: USB-mälupulk; väline kõvaketas või väline välmäluseade; mälukaart, sealhulgas fotoaparaadi ja videosalvesti mälukaart; CD- ja DVD-plaat; nutitelefon, tahvelarvuti või fotoaparaat, kui see ühendatakse arvutiga andmete edastamiseks (ainult laadimiseks ühendamine ei ole andmete edastamine). Seadme koosseisu kuuluvale andmekandjale (arvuti ketas, printeri või koopiaimasina mälu, videovalve salvesti, võrguseadme mälukaart) kohaldatakse ainult 7. peatükki.

1.5. Irdandmekandjaks ei loeta USB kaudu ühendatavaid sisend-, väljund- ja kuvaseadmeid: interaktiivne tahvel, projektor, klaviatuur, hiir, esitluspult, ID-kaardi lugeja, kõlar, dokumendikaamera. Nende ühendamisele kohaldatakse punkti 3.5.

1.6. Kooli andmekandja on kooli soetatud, märgistatud, krüpteeritud ja loendisse (punkt 5.3) kantud andmekandja. Kooli andmekandjad on kantselei varunduskettana kasutatav väline kõvaketas ja infoturbejuhi andmekandja võrguseadmete konfiguratsioonide koopiatega; muu andmekandja kantakse loendisse ainult punkti 2.3 kohase erandi alusel. Isiklik andmekandja on töötaja või muu isiku enda andmekandja.

1.7. Kaitstavad andmed on ainult kahte liiki teave: õpilaste, lapsevanemate ja töötajate isikuandmed (sealhulgas iseloomustused, individuaalsed õppekavad, tugi- ja nõustamisdokumendid, nimedega nimekirjad) ning juurdepääsupiiranguga (AK) dokumendid, sealhulgas kooli süsteemide seadistused ja paroolid. Kaitstavate andmete tunnus on, et failis on konkreetse lapse, lapsevanema või töötaja nimi või juurdepääsupiirangu märged.

Õppematerjalid – esitlused, pildid, tekstid, videod, jaotusmaterjalid, lingid, mis on internetist alla laaditud või õpetaja koostatud – ei ole kaitstavad andmed, kui neis ei ole konkreetse õpilase, lapsevanema või töötaja nime. Neid hoitakse samuti tööarvutis ja prinditakse sealt; irdandmekandjat ei ole nende jaoks vaja.

1.8. Infoturbejuhi ülesandeid täidab kooli haridustehnoloog.

1.9. Kord täiendab kooli infoturbepoliitikat ning täpsustab IT-teenuste kasutamise korda ja IT-halduse korda irdandmekandjate kasutamise küsimustes. Vastuolu korral kohaldatakse käesolevat korda. Paroolidele kohaldatakse autentimiskorda.

1.10. Kord rakendab Eesti infoturbestandardi etalon turbe kataloogi meetmeid, mis on nimetatud kooli infoturvameetmete rakendamise plaanis (edaspidi rakendamise plaan); vastutajad ja tähtsajad on määratud rakendamise plaanis.

1.11. Isikuandmete töötlemisel andmekandjal kohaldatakse lisaks korrale isikuandmete kaitse üldmäärust ja kooli isikuandmete töötlemise nõudeid.

2. Põhimõtte ja lubatud erandid

2.1. Igal töötajal on temale väljastatud kooli sülearvuti, mis on tema ainus tööarvuti; seda võib viia koju ja kõik tööfailid, sealhulgas kaitstavaid andmeid sisaldavate dokumentide mustandid, hoitakse selles. Andmete edastamiseks kasutatakse kooli infosüsteeme, kooli e-posti ja riigiportaale; dokumendid prinditakse otse tööarvutist (punkt 2.4). Kodus tööarvutis koostatud materjale ei ole vaja üle kanda; muus arvutis koostatud või mujalt saadud õppematerjalid saadab töötaja oma kooli e-posti aadressile või laadib tööarvutisse uuesti alla. Töötajad irdandmekandjaid ei kasuta – ei isiklikke ega kooli omi; erandid on punktides 2.2 ja 2.3 ning ühekordne üleviimine punktis 3.3.

2.2. Ainsad lubatud kasutusjuhud on:

2.2.1. kantselei (direktor, sekretär, õppealajuhataja) tööfailide igakuise varukoopia tegemine kooli krüpteeritud välisele kõvakettale (varundusketas); koopia teeb sekretär infoturbejuhi juhiste järgi, ketast hoitakse seifis; reegel kehtib seni, kuni koolis ei ole keskset varundust;

2.2.2. arvutite, võrgu- ja õppeseadmete seadistamine, tarkvara ja püsivara paigaldamine ja uuendamine ning võrguseadmete konfiguratsioonide koopiade hoidmine; seda teeb infoturbejuht kooli andmekandjal, mida hoitakse seifis;

2.2.3. seadme koosseisu kuuluva andmekandja käitlemine seadme kasutuselt kõrvaldamisel 7. peatüki järgi.

2.3. Muul juhul võib irdandmekandjat kasutada ainult direktori kirjalikult kinnitatud erandi alusel (punkt 8.4) infoturbejuhi põhjendatud ettepanekul ja ainult kooli krüpteeritud andmekandjal.

2.4. Printimine. Dokumendid prinditakse otse töötaja tööarvutist tema kabineti printeriga või kontorikombainiga, mille juures töötaja viibib; väljatrükk võetakse kohe kaasa. Printerid seadistab tööarvutitesse infoturbejuht. Printeri või kontorikombaini USB-porti ei kasutata.

2.5. Õpilased. Õpilaste andmekandjaid kooli arvutite ja seadmetega ei ühendata. Õpetaja jälgib selle reegli täitmist klassis.

3. Piirangud

3.1. Töötaja ei ühenda kooli tööarvuti ega muu kooli seadmega ühtegi irdandmekandjat, välja arvatud punktis 2.2 nimetatud juhud, punkti 2.3 kohane erand ja punkti 3.3 kohane ühekordne üleviimine.

3.2. Krüpteerimine. Kooli andmekandjad krüpteerib infoturbejuht BitLocker To Go abil Windows 11 Education väljaandega tööarvutis. Ka punkti 2.3 kohase erandi korral edastatakse andmed ainult krüpteeritud andmekandjal.

3.3. Üleminek. Töötaja, kelle isiklikul andmekandjal on kaitstavaid andmeid, viib need hiljemalt 31.10.2026 üle oma tööarvutisse ja kustutab andmekandjalt; vajaduse korral aitab infoturbejuht. See on ainus lubatud isikliku andmekandja ühendamine tööarvutiga. Töötaja kinnitab üleviimise allkirjaga üleminekunimekirjas (punkt 5.4).

3.4. Isiklikud pilvekontod ei ole korra tähenduses andmekandjad, kuid kaitstavate andmete hoidmine neis on keelatud; andmete üleviimine toimub hiljemalt 31.10.2026 samas korras nagu punktis 3.3. Pilveteenuste kasutamise reeglid kehtestab IT-teenuste kasutamise kord.

3.5. Keelatud on ühendada leitud, teadmata päritolu, kingituseks või tundmatult isikult saadud andmekandjat ning tundmatuid USB-seadmeid, sealhulgas võõraid laadimiskaableid ja reklaamkingitusi. Koolist leitud andmekandja antakse infoturbejuhile ja seda ei ühendata ühegi seadmega.

3.6. Kooli andmekandjaid ei jäeta järelevalveta ega viida koolist välja; neid hoitakse seifis. Kooli andmekandjat ei anta kolmandale isikule infoturbejuhi teadmata.

3.7. Tarkvara paigaldab tööarvutitesse ainult infoturbejuht; töötaja andmekandjalt tarkvara ei paigalda.

3.8. Andmekandja ei ole arhiiv: tööandmete ainsat eksemplari sellel ei hoita. Varundusvahendina kasutatakse ainult punkti 2.2.1 kohast varundusketast.

3.9. Kooli andmeid ei kanta andmekandjale eesmärgiga jätta need isiklikku valdusse pärast tööülesande täitmist või töösuhte lõppemist.

4. Vastutus

4.1. Töötaja ei kasuta töös irdandmekandjaid; hoiab tööfaile tööarvutis ja prindib punkti 2.4 järgi; teeb ülemineku punktide 3.3 ja 3.4 järgi ja kinnitab seda; teatab juhtumitest 6. peatüki järgi.

4.2. Infoturbejuht seadistab printerid kõigis tööarvutites; peab kooli andmekandjate loendit, krüpteerib varundusketta ja hoiab konfiguratsioonide andmekandjat; tööarvutite ettevalmistamisel veendub, et Microsoft Defenderi kaitse on sisse lülitatud; peab üleminekunimekirja; koostab meelepea ja juhendab töötajaid; menetleb 6. peatüki kohaseid teateid, dokumenteerib juhtumid ja rakendab meetmed; korraldab andmete kustutamise ja andmekandjate hävitamise 7. peatüki järgi; kontrollib käesoleva korra täitmist üks kord aastas infoturbe juhtrühma augustikuu koosolekul ja esitab kokkuvõtte direktorile; esitab direktorile ettepanekud korra muutmiseks.

4.3. Direktor kehtestab korra ja selle muudatused ning otsustab erandid (punkt 8.4); tagab vahendid printerite jaoks ja andmekandjate hävitamiseks ning korraldab juhendamise; otsustab jääkriskide aktsepteerimise; otsustab Andmekaitse Inspeksiooni ja andmesubjektide teavitamise (punkt 6.5).

4.4. Õppealajuhataja ja tugispetsialistid tagavad korra täitmise oma valdkonna andmete töötlemisel. Õpetaja jälgib, et õpilased ei ühendaks andmekandjaid kooli seadmetega (punkt 2.5).

4.5. Sekretär registreerib korra ja sellega seotud käskkirjad dokumendihaldussüsteemis, teeb käesoleva korra töötajatele teatavaks, võtab töötajatelt käesoleva korraga tutvumise kohta allkirja, avaldab käesoleva korra kooli veebilehel, teeb kantselei igakuise varukoopia ja hoiab varundusketast seifis (punkt 2.2.1).

4.6. Andmekaitse spetsialist hindab punktide 3.3, 3.4 ja 6.5 kohaseid juhtumeid isikuandmete kaitse seisukohast ja peab nende arvestust.

4.7. Infoturbe juhtrühm vaatab läbi korra täitmise kokkuvõtte ja esitab direktorile ettepanekud.

5. Kontrollimeetmed

5.1. Kahjurvarakontroll. Kõigis kooli tööarvutites töötab Microsoft Defenderi reaaliajakaits. Kui punkti 2.3 kohase erandi alusel või ülemineku käigus (punkt 3.3) ühendatakse tööarvutiga andmekandja, kontrollitakse seda enne failide avamist eraldi (paremklõps andmekandjal failihalduris ja Microsoft Defenderi kontrolli käsk). Kahtluse korral andmekandjat ei avata ja sellest teatatakse infoturbejuhile.

5.2. Vaikeseaded. Microsoft Defenderi kaitse ja programmide automaatkäivituse keeld andmekandjatelt kehtivad Windowsis vaikimisi ja neid eraldi ei seadistata. Tööarvuti ettevalmistamisel veendub infoturbejuht, et kaitse ei ole välja lülitatud ja printer on seadistatud, ning märgib selle tööarvutite loendisse (autentimiskord). Kui töötaja kontolt on autentimiskorra järgi administraatoriõigused eemaldatud, ei saa töötaja kaitset välja lülitada.

5.3. Kooli andmekandjate loend. Infoturbejuht peab loendit, milles on andmekandja liik, märgistus, krüpteerimine, hoiukoht, kasutaja ning märke andmete kustutamise või hävitamise kohta. Andmekandjad märgistatakse nähtavalt. Loend vaadatakse üle kord aastas.

5.4. Üleminekunimekiri. Infoturbejuht peab nimekirja töötajatest, kes on teinud punktide 3.3 ja 3.4 kohase ülemineku, koos kuupäeva ja töötaja allkirjaga, ning esitab kokkuvõtte direktorile pärast üleminekutähtaja möödumist.

5.5. Iga-aastane kontroll. Kord aastas, infoturbe juhtrühma augustikuu koosolekul koos kasutajakontode ülevaatusena, kontrollib infoturbejuht kooli andmekandjate olemasolu ja märgistust, loendi ajakohasust ning korra täitmist. Tulemus vormistatakse kirjalikult.

5.6. Korra rikkumisest teavitab infoturbejuht direktorit. Tagajärjed määratakse töösuhteid reguleerivate õigusaktide ja kooli töökorralduse reeglite järgi.

5.7. Korra kohane kontroll on korralduslik; jääkriskid on arvestatud kooli riskihindamises ja rakendamise plaanis ning nende aktsepteerimise otsustab direktor.

6. Andmekandja kaotamine, vargus ja manipuleerimiskahtlus

6.1. Töötaja teatab viivitamata, hiljemalt samal tööpäeval, infoturbejuhile kooli andmeid sisaldava andmekandja kaotamisest või vargusest; kahtlusest, et andmekandjat on avatud, asendatud või sellega manipuleeritud; tundmatu andmekandja leidmisest koolis; andmekandja

sattumisest kõrvalise isiku valdusse; kahjurvara avastamisest andmekandjal või pärast selle ühendamist.

6.2. Teade esitatakse kooli e-posti teel või telefonitsi; kui infoturbejuht ei ole kättesaadav, siis direktorile. Kiireloomulisel juhul võib teatada suuliselt ja vormistada teate hiljem kirjalikult.

6.3. Heauskne teatamine ei too teatajale kaasa negatiivseid tagajärgi ka siis, kui juhtumi põhjustas tema enda viga.

6.4. Infoturbejuht menetleb teadet infoturbepoliitikas sätestatud korras: dokumenteerib juhtumi, hindab, millised andmed andmekandjal olid, kas need olid punkti 3.2 järgi krüpteeritud, ja juhtumi mõju ning rakendab meetmed (andmekandja isoleerimine, paroolide vahetus, seotud arvutite kontroll, andmete taastamine). Kuni intsidentide arvestuse kasutuselevõtni rakendamise plaani järgi peab ta juhtumite kirjalikku arvestust.

6.5. Kui kaotatud või kõrvalise isiku valdusse sattunud andmekandjal olid isikuandmed, mis ei olnud punkti 3.2 järgi kaitstud, hindab direktor infoturbejuhi ja andmekaitse spetsialisti ettepanekul Andmekaitse Inspeksiooni teavitamise vajadust (teavitamise tähtaeg on isikuandmete kaitse üldmääruse järgi 72 tundi) ja andmesubjektide teavitamise vajadust.

6.6. Kui juhtum on küberintsident, näiteks kahjurvara levik kooli võrgus, teavitab direktor või infoturbejuht CERT-EE-d küberturvalisuse seaduses sätestatud korras ja tähtaja jooksul. Täpsem kord on intsidentidest teavitamise juhendis, mis on ette nähtud rakendamise plaanis.

6.7. Leitud või kahtlast andmekandjat hoiab infoturbejuht eraldi kuni asjaolude selgitamiseni ning seejärel hävitab selle 7. peatüki järgi või tagastab omanikule.

7. Andmete kustutamine ja andmekandja kasutuselt kõrvaldamine

7.1. Andmed kustutatakse andmekandjalt kohe pärast eesmärgi saavutamist; isikuandmeid sisaldavaid faile ei hoita andmekandjal kauem kui toimumiseks vaja.

7.2. Enne kooli andmekandja andmist teisele kasutajale hävitab infoturbejuht krüpteerimisvõtme ja vormindab andmekandja täielikult. Krüpteerimata andmekandjat, millel töödeldi kaitstavaid andmeid, teisele kasutajale ei anta, vaid see hävitatakse punkti 7.3 järgi.

7.3. Kasutuselt kõrvaldatavad mälupulgad ja mälukaardid hävitatakse füüsiliselt, sest väikmälu usaldusväärne ülekirjutamine ei ole tagatud; CD- ja DVD-plaadid purustatakse; väline kõvaketas kirjutatakse üle või hävitatakse füüsiliselt.

7.4. Arvutite, printerite, koopiaimasinate ja muude seadmete koosseisu kuuluvad andmekandjad puhastatakse või hävitatakse enne mahakandmist või utiliseerijale üleandmist: BitLockeriga krüpteeritud ketta puhul hävitatakse võti ja taastatakse tehaseseaded, muul juhul kirjutatakse ketas üle või hävitatakse füüsiliselt.

7.5. Kustutamine ja hävitamine dokumenteeritakse mahakandmisaktis või andmekandjate loendis: märgistus, meetod, kuupäev, tegija. Utiliseerijalt võetakse üleandmisakt, milles on märgitud andmekandjate hävitamine.

8. Rakendussätted

8.1. Kord jõustub direktori käskkirja allkirjastamisel; irdandmekandjate kasutamise keeld (punkt 2.1) kehtib sellest päevast.

8.2. Töötajaid puudutavad tähtjad: kaitstavate andmete üleviimine isiklikelt andmekandjatelt ja isiklikelt pilvekontodelt – hiljemalt 31.10.2026 (punktid 3.3 ja 3.4); käesolev kord tehakse töötajatele teatavaks PINALi kaudu – hiljemalt 31.10.2026.

8.3. Korra rakendamise muude tegevuste (printerite seadistamine tööarvutites, varundusketta krüpteerimine ja loendisse kandmine, meespea ja juhendamine, hävitamisnõuete kohaldamine) tähtjad on määratud infoturvameetmete rakendamise plaanis.

8.4. Erandi korrast kinnitab direktor kirjalikult infoturbejuhi põhjendatud ettepanekul; erandid ja nendega seotud riskid kajastatakse riskihindamises ja rakendamise plaanis.

8.5. Käesolev kord vaadatakse üle vähemalt üks kord aastas ning pärast olulisi muudatusi kooli infosüsteemides või õigusaktides; ülevaatus korraldab infoturbejuht, muudatused kehtestab direktor käskkirjaga.