Tallinna Ülikool
Digitehnoloogiate Instituut

Kolmandas kooliastmes ja gümnaasiumis kasutatavate e-keskkondade turvalisus ja privaatsus

Magistritöö

Autor: Kati Liik
Juhendaja: Birgy Lorenz, Ph.D.

Autor: ……. "…" …….. 2017
Juhendaja: ……. "…" …….. 2017
Instituudi direktor: ……. "…" …….. 2017

Tallinn 2017

Autorideklaratsioon

Deklareerin, et käesolev magistritöö on minu töö tulemus ja seda ei ole kellegi teise poolt varem kaitsmisele esitatud. Kõik töö koostamisel kasutatud teiste autorite tööd, olulised seisukohad, kirjandusallikatest ja mujalt pärinevad andmed on viidatud.

.....	.....
(kuupäev)	(autor)

Lihtlitsents lõputöö reprodutseerimiseks ja lõputöö üldsusele kättesaadavaks tegemiseks

Mina, Kati Liik (sünnikuupäev: 08.05.1977)

1. Annan Tallinna Ülikoolile tasuta loa (lihtlitsentsi) enda loodud teose "Kolmandas kooliastmes ja gümnaasiumis kasutatavate e-keskkondade turvalisus ja privaatsus", mille juhendaja on Birgy Lorenz, säilitamiseks ja üldsusele kättesaadavaks tegemiseks Tallinna Ülikooli Akadeemilise Raamatukogu repositooriumis.

2. Olen teadlik, et punktis 1 nimetatud õigused jäävad alles ka autorile.

3. Kinnitan, et lihtlitsentsi andmisega ei rikuta teiste isikute intellektuaalomandi ega isikuandmete kaitse seadusest tulenevaid õigusi.

Tallinnas, _____

allkiri ja kuupäev

Sisukord

Töös kasutatavad põhimõisted

Autentimine on kinnituse andmine olemi väidetava identiteedi, tunnusomaduse või päritolu õigsusele; protsess, millega üks kasutaja, süsteem vm olem saab kontrollida teise olemi väidetava identiteedi tõesust, tavaliselt mingi esitatud spetsiifilise teabe (näiteks parooli), eseme (näiteks kiipkaardi vm turvatõendi) või eristava püsitunnuse (biomeetriku) alusel (Cybernetica AS, 2011-2017).

Digijälg ehk digiaedik on inimeste interneti külastuste käigus neist maha jääv tegevuste logi (Andrejevitš, 2009).

Digipädevus tähendab suutlikkust rakendada info- ja kommunikatsioonitehnoloogiat (edaspidi IKT) enesekindlalt, kriitiliselt ja loominguliselt oma tööga, töövalmidusega, õppimisega, meelelahutusega ja ühiskonda kaasatusega seonduvate eesmärkide täitmiseks (European Parliament, 2006).

E-õpe on IKT kaasabil toimuv õppetegevus, mis leiab aset nii klassiruumis, kui ka väljaspool klassiruumi või ametlikku õppetundi (Haridustehnoloogia sõnastik, kuupäev puudub).

E-õppe keskkond ehk õpihaldussüsteem on veebipõhine serveritarkvara õppesisu (nt õppematerjalid, harjutused, testid) ja õppeprotsesside (nt juhendamine, tagasiside, arutelud, kodutööd, rühmatöö, hindamine) haldamiseks (Haridustehnoloogia sõnastik, kuupäev puudub).

Kahetasandiline autentimine - kasutaja turvaliseks autentimiseks kasutatakse lisaks esimesele turvategurile (nt parool) ka teist turvategurit (nt paroolikaart või lühisõnumiga mobiilile saadetav kood) (Võrguvara.ee[1]).

Konfidentsiaalsus tähendab, et andmeid peavad saama käidelda vaid selleks volitatud inimesed ja protsessid (Riigi Infosüsteemi Amet, kuupäev puudub, b).

Käideldavus tähendab andmete õigeaegset ja mugavat kättesaadavust ning kasutatavust. Andmeid peab kasutada saama nii volitatud inimene, kui

[1] https://www.vorguvara.ee/turvaline-autentimine-1

andmetöötlusprotsess. Vastavalt kasutaja soovile peab olema võimalik andmeid kasutada erinevates vormingutes (Riigi Infosüsteemi Amet, kuupäev puudub, b).

Privaatsus (informatsiooniline privaatsus) tähendab isiku õigust infokeskkonnas ise otsustada, kes ja mil määral saavad juurdepääsu tema teabele ja seda kasutada (Steeves, 2009).

Tervikluse all mõistetakse andmete põhinemist algallikal ning veendumust, et need pole hiljem muutunud või neid pole volitusteta muudetud. Andmed peavad olema terviklikud, õiged ja sidusad. Oluline on ka andmete muutmise jälitatavus. Peab olema tuvastatav, kes, millal ja miks andmeid sisestas, muutis või kustutas (Riigi Infosüsteemi Amet, kuupäev puudub, b).

Turvalisus e-õppes tähendab, et õppematerjalid on kättesaadavad ja rikkumata kõikidele volitatud kasutajatele sel hetkel, kui nad neid vajavad (Adams & Blandford, 2003).

Turvaintsident on planeerimatu sündmus, millega kaasneb andmete või muude infovarade käideldavuse, tervikluse või konfidentsiaalsuse kadu või tekib oht nende kadumiseks (Riigi Infosüsteemi Amet [RIA], kuupäev puudub).

Õppeinfosüsteem, näiteks eKool, on infosüsteem, mis ühendab kõiki õppetööga seotud osapooli: koolijuhte, õpetajaid, klassijuhatajaid, õpilasi, lapsevanemaid. Süsteemi tähtsaimaks osaks on klassipäevik, milles on õpetaja poolt sisestatud hinded, tunni sisu kirjeldused, kodused ülesanded, puudumised, hilinemised, märkused ning kontrolltööde ajad (eKool[2]).

2 https://ee.ekool.eu/index_et.html

Sissejuhatus

Õpetaja võttis kasutusele uue e-keskkonna, kuid ei tutvustanud selle kasutamise põhimõtteid ja turvalisuse- ja privaatsuse sätteid õpilastele. Õpilased pidid keskkonda sisestama essee, milles mõni õpilane oli käsitlenud ka oma isiklikke probleeme. Hiljem avastasid õpilased, et nende esseed on avalikult veebist kõikidele kättesaadavad.

See on vaid üks, väga lihtsustatud näide sellest, kuidas digipuhanguga võetakse kasutusele erinevaid e-keskkondi, uurimata või lõpuni aru saamata nende turvalisuse ja privaatsuse sätetest. Kindlasti oleks sellises olukorras võinud õpetaja õpilast rohkem juhendada, tuua välja keskkonna puudused ja viidata võimalikele ohtudele. Kuid kas õpetaja ise tutvus nende sätetega? Kui oleks tutvunud, kas ta oleks osanud ohtudele või süsteemi eripäradele tähelepanu pöörata? Ühelt poolt on surve e-keskkondade kasutuselevõtuks olemas, kuid turvalisuse pool kipub selle juures jääma madalama tähelepanu alla.

Haridusvaldkonna digitaliseerumise areng algas 1995. aastal, kui 14. veebruaril avaldati ajalehe Rahva Hääl veergudel tolleaegse suursaadiku Toomas Hendrik Ilvese mõte Kultuuri- ja Haridusministeeriumile, varustada kõik Eesti keskkoolid arvutitega. Ettepaneku rakendamiseks toimus järgmisel aastal, 18. detsembril, Tallinnas, Rahvusraamatukogus Tiigrihüppe Sihtasutuse loomiseks esimene koosolek (Eesti Hariduse ja Teaduse Andmesidevõrk, kuupäev puudub). Tänaseks on Tiigrihüppe Sihtasutusest saanud Hariduse Infotehnoloogia Sihtasutuse (edaspidi HITSA) Innovatsioonikeskus, kus siiani tegutsetakse erinevate innovatsiooniprojektidega (Hariduse Infotehnoloogia Sihtasutus, kuupäev puudub). Digitaliseerumise toetamiseks loodi 2016. aastal Digipöörde programm (Haridus- ja Teadusministeerium [HTM], 2015) ja üldhariduskoolide digitaristu kaasajastamiseks toetusmeede (Majandus- ja Kommunikatsiooniministeerium [MKM], 2016), mille raames muretsetakse koolidele IKT baasvarustust ja luuakse uusi traadita interneti võimalusi. Samas pole seni piisavalt tähelepanu pööratud digitaliseerumisega kaasnevale e-keskkondade turvalisele kasutamisele või turvalisusega seotud digipädevuste tõstmisele.

Turvalisusel on mitmeid erinevaid tahke, osad neist kuuluvad infotehnoloogia valdkonda, näiteks võrguturve, seadmete füüsiline turve, paroolide turvalisus jms, mille eest vastutavad tavaliselt IT-juhid või teised IT-töötajad. Kuid, kui me räägime hariduses kasutatavatest keskkondadest, siis peaksid koolijuhid, õpetajad ja haridustehnoloogid olema piisavalt pädevad, et hinnata õppetöös kasutusele võetava rakenduse ohutust selle kasutajatele. Enne keskkonna kasutuselevõttu peaks olema nii õpetajale kui õpilasele selge, kas selle kasutamine on õppetööks turvaline ja milliseid ohte keskkonna erinevad kasutamise võimalused kaasa tuua võivad.

Töö eesmärk on läbi uurimisküsimuste jõuda soovitusteni, millele koolides kasutusel olevate e-keskkondade turvalisuse- ja privaatsussätete juures tähelepanu pöörata.

Seega on antud magistritöö uurimisküsimusteks:

- Kas Eestis kehtivatesse digipädevuste nõuetesse on sisse kirjutatud turbe teemalisi pädevusi?
- Milliseid e-õppe keskkondasid Eesti koolides kasutatakse ja milliseid probleeme on nende kasutamisel ette tulnud?
- Millised on nende keskkondade turvalisuse- ja privaatsuse sätted ning kuidas neid sätteid kasutada, et oma turvalisust ja privaatsust kaitsta?

Töö koosneb teoreetilistest ja empiirilistest osadest, kuuest peatükist. Esimeses peatükis uuritakse ootuseid õpilaste ja õpetajate digipädevustele turvalisuse valdkonnas. Teises peatükis antakse ülevaade e-õppe keskkondadest üldiselt, erinevat tüüpi e-keskkondade positiivsetest ja negatiivsetest külgedest ning turvalisuse ja privaatsuse temaatikast üldiselt. Kolmandas peatükis tuuakse välja uurimismeetodid ja kirjeldatakse valimit. Neljandas peatükis esitatakse ankeetküsitlusega selgunud uurimuse tulemused. Viiendas peatükis analüüsitakse ankeetküsitlusega selgunud enamkasutatavate e-keskkondade turvalisuse- ja privaatsuse sätteid. Analüüsitakse, kas enamkasutatavate e-keskkondade kasutustingimustes on käsitletud Euroopa Liidu andmekaitse direktiivis (1995) nimetatud levinumaid privaatsuse eiramise viise. Lisaks koostatakse detailne turvalisuse ja privaatsuse sätete ülevaade, milles tuuakse välja enamkasutatavate keskkondade turvalisuse ja privaatsuse sätted, vaikesätted ja soovitused nende sätete muutmiseks. Kuues peatükk sisaldab arutelu ja järeldusi. Lisaks põhiosadele sisaldab töö 2 joonist, 5 tabelit, inglisekeelset resümeed ja 2 lisa.

1 Õpilaste ja õpetajate digipädevused ja koolide digiküpsuse hindamine turvalisuse valdkonnas

Eestis on loodud mitmeid arengukavasid, mis puudutavad tehnoloogia arengut ja ka turvalisust. Näiteks Eesti infoühiskonna arengukava 2020 (MKM, 2014b) järgi on infoühiskonna teadlikkuse programmi raames järjepidevalt tõstetud inimeste teadlikkust infoühiskonna võimalustest ja ohtudest, pannes erilist rõhku turvalise netikäitumise oskustele. Samuti on arengukavas kirjas, et infoühiskonna areng ei tohi vähendada kasutajate turvatunnet. Infoühiskonna arengukava on seotud ka Küberjulgeoleku strateegiaga 2014 – 2017 (MKM, 2014a), milles on samuti välja toodud, et tuleb luua tingimused selleks, et IKT võimalusi saaks tõhusalt ja turvaliselt kasutada. Infoühiskonna arendamine ja küberjulgeoleku tagamine peavad toimima paralleelselt ja ühtsena (MKM, 2014b).

Ka küberjulgeoleku arengukava elluviimine edendab Eesti IKT lahenduste kasutuselevõtu keskkonda. Näiteks on küberjulgeoleku strateegia rakendamiseks tegelenud Politsei- ja Piirivalveamet küberkuritegevuse ohutuse alase teadlikkuse tõstmisega, mille käigus on muu hulgas loodud veebikonstaabli ametikohad. Veebikonstaabli ülesanne on tõsta inimeste teadlikkust Interneti turvalisuse osas ning kaitsta lapsi ja noori Internetis (MKM, 2014a).

Eesti elanike IKT alaste oskuste ja teadlikkuse tõstmise eesmärgi osas on hariduse valdkonnas peamine roll Eesti elukestva õppe strateegial 2014–2020 (Haridus- ja Teadusministeerium [HTM], 2014), mille võtmes on haridus- ja teadusvaldkonnale järgmised ootused:

- *IKT lõimimine kõigi erialade õppekavadesse kõigil haridustasemetel;*
- *IKT baasoskuste tagamine põhikooli lõpuks;*
- *IKT erialadel õpilaste arvu suurendamine ja õppekvaliteedi parandamine;*
- *teadlaste pealekasvu suurendamine IKT erialadel, et tagada koolitusmahu ja teadustöö kvaliteedi kasv;*
- *IKTga seotud teadustööde mahu kasv kõigi kõrghariduse erialade lõikes* (MKM, 2014a).

2015. aastal on Euroopa Komisjoni teadustalitus Teadusuuringute Ühiskeskus välja andnud *DigCompOrg* Euroopa raamistiku (Kampylis, Punie, & Devine, 2015). Raamistiku väljatöötamine oli üks osa 2014. aasta detsembrist kuni 2017. aasta juunini läbiviidavast innovaatilise hariduse edendamise projektist *InnovativEdu*. Selle projekti eesmärkideks on:

- *töötada välja digipädevate haridusorganisatsioonide Euroopa võrdlusraamistik DigCompOrg koos selle juurde kuuluva enesehindamise küsimustikuga;*
- *töötada välja õpetajate digipädevuse raamistik koos selle juurde kuuluva enesehindamise küsimustikuga;*
- *analüüsida digitehnoloogiate haridus- ja koolitussüsteemidesse lõimimise ja innovaatilise kasutamise tõhusaid poliitikamudeleid;*
- *esitada teaduslikke tõendeid õpianalüütika kasutamise kohta hariduses ja koolituses ning sellest tulenevate võimalike hariduspoliitiliste järelduste kohta* (Kampylis et al., 2015).

Raamistiku eesmärgid ei ole otseselt seotud e-õppe keskkondade turvalisuse teemadega, kuid siiski puudutatakse neid teemasid raamistiku seitsmest teemaelemendist kolmes. Näiteks õpetamise ja õppimise tegevuste teema all käsitletakse organisatsiooni vastutust õpilaste ja koolipersonali turvalisuse ning heaolu ees digivahendite kasutamisel. Õpilaste ja koolipersonali digipädevused hõlmavad endas oskusi kaitsta enda turvalisust ja privaatsust digivahendite kasutamisel, samuti ka teadlik olemist erinevatest esineda võivatest ohtudest. Koostöö ja võrgustumise all käsitletakse erinevate e-keskkondade ja meediaplatvormide kasutamist, mis peavad võimaldama turvalist suhtlust nii kooli sees kui väljaspool. Taristu valdkonnas käsitletakse erinevaid dokumente, strateegiaid ja põhimõtteid, mis aitavad tagada õpilaste ja koolipersonali privaatsuse ja andmete turvalisuse, samuti keskkondade ning seadmete ohutu kasutamise (Kampylis et al., 2015).

Ka Eestis on nii õpilaste kui õpetajate digipädevuste tõstmiseks käivitatud erinevaid programme, mille kaudu toimub Eesti elukestva õppe strateegia rakendamiseks vajalike meetmete ja tegevuste planeerimine, eelarvestamine, elluviimine ja aruandlus. Digipädevusi puudutab neist kõige enam Digipöörde programm.

Programmi eesmärk on: *„rakendada õppimisel ja õpetamisel kaasaegset digitehnoloogiat otstarbekamalt ja tulemuslikumalt, parandada kogu elanikkonna digioskusi ja tagada ligipääs uue põlvkonna digitaristule“* (HTM, 2015).

Kirjeldatud riiklikest strateegiatest ja programmidest ilmnevad selgelt sõnastatud ootused õpilaste ja õpetajate digipädevuste kasvuks. Seega uuritakse järgmises kolmes alapeatükis milliseid turvalisuse valdkonna pädevusi täpsemalt õpilastelt ja õpetajatelt ja ka koolidelt üldiselt eeldatakse.

1.1 Õpilaste digipädevuste tõstmine turvalisuse valdkonnas

Lisaks digipädevusi tõstvatele programmidele on Eestis aastatel 2006 – 2016 läbi viidud, või alles käimas, hulgaliselt turvalisust puudutavaid programme, mis aitavad nii õpilastel kui õpetajatel oma digipädevusi tõsta just turvalisuse valdkonnas. Põhjaliku ülevaate sellistest programmidest saab Birgy Lorenzi doktoritöö lisast 3 (Lorenz, 2017). Näiteks on üheks selliseks programmiks 2012. aastal loodud Targalt Internetis programm. Selle programmi raames korraldatakse konverentse, kampaaniaid, võistlusi, antakse välja õppematerjale, korraldatakse laagreid jne. Käivitatud on telefoni abiliin. Programmi eesmärgiks on: „*laste ja lapsevanemate targem internetikasutus ning laste seksuaalset ärakasutamist esitava sisuga materjalide leviku tõkestamine internetis*“ (Targalt Internetis, kuupäev puudub).

Digipöörde programmi raames viidi Tallinna Ülikooli ja Tartu Ülikooli teadurite poolt läbi *DigCompOrg* Euroopa raamistiku hindamismudeli uuring (Laanpere, Pata, Luik, & Lepp, 2016), mille tulemusena töötati HITSAs 2016. aasta aprillis välja õppijate digipädevuste mudel (HITSA, 2016). Mudel koostati *DigiCompOrg* raamistiku alusel, arvestades ka turvalisuse aspekte, nagu intellektuaalse omandi kaitse ja litsentside järgimine, oma identiteedi kaitsmine ja IKT turvaline kasutamine. Samuti lähtuti mudeli koostamisel põhikooli riiklikus õppekavas (2014) ja gümnaasiumi riiklikus õppekavas (2014) toodud temaatikatest: tehnoloogia ja innovatsioon; teabekeskkond; informaatika ja uurimistöö alused (Mets, Nevsky, Pedaste, & Laanpere, 2016).

Seega seisnevad kokkuvõtvalt turvalisuse valdkonnas digipädevuste ootused õpilastele selles, et nad tunneksid potentsiaalseid digikeskonna ohtusid ning oskaksid kaitsta oma identiteeti, isikuandmeid ja privaatsust. Järgmises alapeatükis uuritakse,

kas ka õpetajatele on turvalisuse valdkonna pädevuste osas ootusi.

1.2 Õpetajate digipädevuste tõstmine turvalisuse valdkonnas

Sarnaselt õppijate digipädevuste mudelile on innovaatilise hariduse edendamise projekti *InnovativEdu* (Kampylis et al., 2015) raames plaanis välja töötada ka õpetajate digioskuste enesehindamise keskkond. Dokument on praegu alles mustandi kujul (European Commission, 2017). Hetkel juhindutakse 2008. aastal koostatud õpetajate digipädevuste standardist (International Society for Technology in Education [ISTE], 2008), mille neljas punkt puudutab ka turvalist digikäitumist: *õpetajad mõistavad arenevas digikultuuris nii kohalikke kui globaalseid kitsaskohti ja vastutust ning käituvad oma professionaalses tegevuses seaduslikult ja eetiliselt. Õpetajad soovitavad, edendavad ja õpetavad digitaalse teabe ja tehnoloogia turvalist, seaduslikku ja eetilist kasutamist, sh autoriõiguste ja intellektuaalse omandi põhimõtete järgimist ning asjakohast allikatele viitamist. Õpetajad on eeskujuks digitehnoloogia ja teabe kasutamisega seotud etiketi järgimisel ja edendavad vastutustundlikku suhtlust digikeskkonnas* (ISTE, 2008).

Hetkel on *InnovativEdu* projekti raames sarnaselt õpilaste digipädevuste mudelile väljatöötamisel ka uus õpetajate digipädevuste mudel *Proposal for a European Framework for the Digital Competence of Educators* (European Commission, 2017).

Kui võrrelda ootusi õpilaste ja õpetajate digipädevustele, siis need üldiselt kattuvad - see, mida peab oskama õpilane, peab õpetaja oskama toetada ja nõu anda. Järgmises alapeatükis uuritakse millistel tasemetel saavad koolid enda digiküpsust hinnata.

1.3 Koolide digiküpsuse hindamine turvalisuse valdkonnas

Üheks levinud koolide e-ohutuse hindamise raamistikuks on *European Schoolneti* poolt loodud *e-safety label*. Täites küsimustiku, saab kool tagasiside, milline on tema e-turvalisuse tase võrreldes teiste koolidega ja vastavalt tasemele on võimalik saada kas kuld-, hõbe- või pronksmärk. Küsimustikust leiab küsimusi kooli infrastruktuuri, võrgu, kasutatavate seadmete, isikuandmete kaitse, kasutatavate infosüsteemide ja e-õppekeskkondade, paroolihalduse, kooli poliitikate ja dokumentatsiooni ja parimate e-ohutuse praktikate kohta (European Schoolnet, kuupäev puudub).

Euroopa Komisjoni Teadusuuringute Ühiskeskuse poolt välja antud *DigCompOrg* raamistik võimaldab hinnata ka kooli edusamme e-õppe tehnoloogiate õppetöösse lõimimisel ja tõhusal kasutamisel (Kampylis et al., 2015).

Tallinna Ülikoolis on selle raamistiku alusel loodud Eesti enda koolide hindamisvahend Digipeegel. Digipeegliga saavad Eesti koolid enda digiküpsust hinnata digitaristu, õpikäsituse ja muutuste juhtimise valdkondades. Digiküpsuse enesehindamise mudel on loodud kooli sisehindamise ja juhtimisinstrumendina, mistõttu on koolil mõistlik seda kasutada ausalt ja enesekriitiliselt. Enesehindamist saab läbi viia Digipeegli veebilahenduse abil ning hindamistulemused saab muuta kättesaadavaks koolipidajale. Vastavalt vajadusele saab kooli digiküpsuse hinnangut avalikustada diagrammi koondatud üldinfona kogu avalikkusele. Kogutud enesehindamise tulemuste alusel ei seata koole pingerea alusel ritta. Küll aga saab iga kool Digipeegli abil võrrelda enda digiküpsust teiste koolidega (Laanpere, 2016).

Digitaristu osas saavad koolid anda hinnangu ka oma võrgule ja digiturbele ning tarkvarale, teenustele ja infosüsteemidele. Digiturbe osas on jooniselt 1 näha, et alles „E“ tasemele jõudnud kool peaks olema võimeline juhtima IT turvariske tasemel, mis võimaldab ennetada turvaintsidente. Samas, juba „B“ taseme kool kasutab üksikuid e-õppe keskkondasid, mille kasutamisel võib juba turvaintsidente ette tulla.

3. DIGITARISTU				
3.1. Võrk ja digiturve				
Kooli arvutivõrgu ja digiturbe kvaliteet - kaasaegsed võrgulahendused ja nendele vastavate digiturbe reeglite olemasolu ja rakendamine. IT ja haridustehnoloogilise kasutajatoe tagamine.				
A - tase	**B - tase**	**C - tase**	**D - tase**	**E - tase**
Üksikutes kooliruumides on Wifi, interneti välisühendus on rahuldav kuni 30 samaaegse kasutaja puhul	Kooli ruumidest enamus on Wifiga kaetud, aga see ei võimalda veel kõigi õpilaste samaaegset võrgukasutust.	Terve kool on kaetud uusima põlvkonna kiire Wifi-võrguga ja välisühenduse kiirust on tõstetud, võimaldades terve koolipere samaaegset intensiivset võrgukasutust, eraldi alamvõrgud on rajatud õpetajatele, õpilastele ja kooli külastajatele.	Kooli võrgulahendus kasutab moodsat ja turvalist ühekordse sisselogimise lahendust ja ühtset kasutajahaldust erinevate infosüsteemide koostalitluseks, kooli võrguliiklust monitooritakse ja analüüsitakse regulaarselt.	Kool tegeleb pidevalt uute võrgulahenduste katsetamise ja arendamisega, nõustades teisi piirkonna koole, asutusi ja ettevõtteid võrgutehnoloogia alal. Toimib IT turvariskide juhtimine tasemel, mis võimaldab intsidentide ennetamist.

3.5. Tarkvara ja teenused, infosüsteemid				
Tarkvara ja e-teenused ning infosüsteemid. Kooli liikumine pilvelahenduste ja koosvõimeliste infosüsteemide suunas, mis toetab õpetajate ja õpilaste igapäevast õppekorraldust ja muutunud õpikäsituse juurutamist.				
A - tase	**B - tase**	**C - tase**	**D - tase**	**E - tase**
Kooli tasandil korraldatakse vaid üksikute administratiivsete e-teenuste kasutamist (nt e-päevik, õppeinfosüsteem, EHIS, kooli koduleht jne).	Kooli tasandil on hakatud juurutama üksikuid lisateenuseid (nt veebipõhised õpikeskkonnad, blogid, raamatukogu infosüsteem).	Kool tagab kooli töötajatele ja õpilastele ligipääsu hästitoimivatele e-teenustele ja infosüsteemidele, mille kasutamist kool monitoorib ja mille kohta pakutakse vajadusel ka sissejuhatavat koolitust koos juhendmaterjalidega. Lisaks administratiivsetele teenustele (e-päevik, õppeinfosüsteem, dokumendihaldus, koduleht) veebipõhised õpikeskkonnad, õppematerjalide ja uurimistööde repositooriumid jm.	Koolis toimib mugav ja mitmekülgne pilvelahendus või infosüsteem, kuhu on ühendatud erinevaid koosvõimelised e-teenuseid. Pidevalt katsetatakse uusi lahendusi, muuhulgas õpilaste uurimistööde ja arendusprojektide kaudu.	Koolis välja arendatud e-teenuste ja infosüsteemide integreeritud lahendus on eeskujuks teistele koolidele, seda lahendust levitatakse koolituste ja nõustamise kaudu.

Joonis 1. Digitaristu hindamine Digipeegli abil (Laanpere, 2016)

Eeltoodust nähtub, et oodatavad digipädevused on üldiselt nii õpilastele, õpetajatele kui ka koolidele kirjeldatud. Õpilased peavad olema teadlikud e-keskkondade ohtudest ja peavad oskama oma privaatsust kaitsta ning õpetajad peavad olema võimelised soovitama õpilastele turvalisi keskkondi ja juhendama neid turvateadlikult kasutama.

Et saada teada milliseid probleeme e-keskkondade kasutamine võib kaasa tuua ja millega toimetulekuks on eelkirjeldatud digipädevused vajalikud, uuritakse järgmises peatükis millist tüüpi e-õppe keskkondasid kasutatakse ning milliste turvalisuse ja privaatuse probleemidega peab arvestama.

2 E-õppe keskkonnad ning nende turvalisus ja privaatsus

Üha enam kasutatakse õpetamisel digivahendeid ja e-keskkondasid, mis annavad võimaluse viia läbi õppimist e-õppena nii ühes õpperuumis, kui ka interneti vahendusel. Alljärgnevalt uuritakse millised võivad olla e-keskkondades ette tulevad turvalisuse ja privaatsuse probleemid ja milliseid e-keskkondasid e-õppes kasutatakse.

2.1 Turvalisus ja privaatsus

Adams & Blandford (2003) on lihtsalt ja arusaadavalt turvalisuse põhikomponente - käideldavus, terviklus ja konfidentsiaalsus silmas pidades defineerinud turvalisuse e-õppe kontekstis: turvalisus e-õppes tähendab, et õppematerjalid on kättesaadavad ja rikkumata kõikidele volitatud kasutajatele sel hetkel, kui nad neid vajavad. Steeves (2009 lk 199) lisab, et informatsiooniline privaatsus tähendab isiku õigust infokeskkonnas ise otsustada, kes ja mil määral saavad juurdepääsu tema teabele ja seda kasutada.

„Privaatsusõiguse rikkumisega võib kaasneda mitmeid ebasoovitavaid tagajärgi isiku jaoks, näiteks identiteedi vargus ja seeläbi juurdepääs isiku varadele või talle määratud hüvedele, ebaõiglus, mida tekitatakse teatud info ärakasutamise või ebavõrdse kohtlemise kaudu, samuti eneseväärikuse riivamine“ (Murumaa-Mengel, Pruulmann-Vengerfeld & Laas-Mikko, 2014).

Näiteks võib noorele inimesele tulevikus probleeme põhjustada e-õppe keskkonda üleslaetud arvamuslood, esseed, kommentaarid või muud kas isiklikke veendumusi, harjumusi, nõrkuseid sisaldavad või hoopis teiste suhtes kriitilised või muud moodi ebasobivad mõtteavaldused. Nagu ülal kirjeldatud probleemidest nähtub, hakkavad andmed avalikustades kohe oma elu elama ning võivad tulevikus saada näiteks takistuseks teatud töökohtadele kandideerimisel või kujundada isiku suhtes põhjendamatult negatiivseid eelarvamusi.

Tartu Ülikoolis Murumaa-Mengel et al. (2014) poolt koostatud uuringu „Privaatsusõigus inimõigusena ja igapäevatehnoloogiad” teoreetiliste ja empiiriliste lähtealuste kokkuvõttes tuuakse välja, et selline avalikkus, mille on tekitanud

inimestele sotisaalvõrgustikud, teevad avaliku elu ja privaatse elu piirid ürna ähmaseks. Võrreldes eeltoodut sellega, kuidas inimesed tavaliselt avalikus ruumis (näiteks tänavatel, ühistranspordis, kaubanduskeskustes jm) käituvad, saab välja tuua neli peamist tunnust, mis eristab privaatsust Internetikeskkonnas füüsilisest, avaliku ruumi privaatsusest:

- *püsivus. 15-aastasena tehtud teod ja väljaöeldud arvamused on kättesaadavad ja nähtavad inimese vanemaks saades, arvestamata seda, et inimese hoiakud ja hinnangud on muutunud;*
- *otsitavus. Avaldatud infot on võimalik vähese vaevaga internetiavarustest üles leida;*
- *kopeeritavus. Digitaalne info on kergesti kopeeritav ning seega on võimalik infot ühest kontekstist teise tõsta, samuti algset infot märkamatult moonutada;*
- *nähtamatu auditoorium. Vahendatud avalikkuses ei näe me enda jälgijaid ning eelmised kolm tunnust muudavad piilujatele kättesaadavaks aja ja ruumi, milles nad ise osalised olnud ei ole* (Muruma-Mengel et al., 2014).

Eurobaromeetri eriuuringus (Eurobaromeetri eriuuring 359, 2011) uuriti inimeste suhtumist privaatsusesse ja sellega seotud harjumusi. Näiteks oli üheks küsimuseks see, kas inimesed tavaliselt loevad keskkondade privaatsuse- ja kasutustingimusi või mitte. Kümnest vastanust kuus ütlevad, et nad loevad neid tingimusi. Kolmandik neist ütleb, et nad saavad nendest ka aru. Veerand küll loeb, kuid ei saa neist aru ja sama paljud tunnistavad, et nad ei loe neid tingimusi üldse. Peaaegu iga kümnes ignoreerib kasutustingimusi ja üks kahekümnest ütleb, et ei oska neid kusagilt leida. Vastanute hulgas, kes ei ole privaatsussätteid muutnud, on eestlased Euroopas esikohal vastusega „ma ei tea, kuidas seda teha". Nendelt vastanutelt, kes ei loe privaatsustingimusi, küsiti ka põhjuseid, miks nad seda ei tee. Eestlaste seas kujunesid vastuste protsendid järgmiselt: 52% leidis, et juba see on piisav, et keskkonnal on sellised tingimused üldse kirjeldatud. 20% vastanutest uskus, et andmete lekkimisel kaitsevad seadused neid nagunii, hoolimata sellest kas kasutustingimustega oldi nõustutud või turvasätted müütamata. 24% vastanuid leidis vastupidist, et isegi, kui turvalisuse sätteid muuta, ei arvesta keskkonnad sellega nagunii (Eurobaromeetri eriuuring 359, 2011).

Nendelt vastajatelt, kes tavaliselt loevad privaatsus- ja kasutustingimusi, uuriti ka

seda, kas nad on pärast nende lugemist jätnud teenuse kasutamata. Tulemusteks oli, et üle kahe kolmandiku vastanutest on muutnud pärast tingimuste lugemist oma suhtumist - pooled muutusid oma isikuandmete avaldamisel ettevaatlikumaks ja pooled on vähemalt korra otsustanud teenuse kasutamisele võtust loobuda. Kümnest kolm vastajat ei ole teenuse kasutuselevõtust loobunud pärast privaatstingimuste lugemist (Eurobaromeetri eriuuring 359, 2011).

Lorenz ja Kikkas (2014) toovad oma uurimuses välja õpilaste suhtumise internetist nende kohta leiduva info osas. Näiteks arvavad õpilased, et see info, mis on kellegi teise poolt nende kohta veebi üles laetud, ei mõjuta neid. Või, et nad võivad küll laadida enda kohta internetti igasugust infot ja see ei mõjuta neid hiljem kuidagi, või, et see info ei huvita kedagi. Teine osa õpilasi, kes juba saavad aru, et internetist nende kohta leitav info võib neid tulevikus mõjutada, näiteks tööle saamisel, püüavad oma kohta leiduvat negatiivset infot (digijälge) vähendada. Näiteks otsivad võimalusi selle info kustutamiseks. Negatiivse info mõju vähendamiseks saab ka ise lisada enda kohta veebi palju positiivset informatsiooni. Sellega taandub negatiivne info veebiajaloos kaugemale ja ei tule enam otsingutes nii kiirelt ja lihtsalt välja (Lorenz & Kikkas, 2014).

Selline strateegia on küll üks võimalus vähendada negatiivse info mõju, kuid siiski suurendab selline käitumine oluliselt muus osas inimese digijälge ja näiteks Oolo ja Siibaki (2013) arvates on kõige lihtsam viis oma privaatsuse kaitsmiseks jagada internetikeskkonnas enda kohta võimalikult vähe infot. Kuigi ka see ei ole väga tõhus soovitus, sest inimesed arvavadki, et nad sisestavad vähe infot ja väikesele ringkonnale. Inimesed ei taju, et tegelikult on jagatud info kättesaadav oluliselt suuremale hulgale, ega mõtle sellele, et järgmisel sekundil, kui nad on oma info avaldanud, võib see olla juba kopeeritud mujale. Samuti viitavad Oolo ja Siibak (2013) oma dokumendis probleemidele, kus erinevates veebikeskkondades on küll olemas võimalused turvalisuse ja privaatsussätete rangemaks seadistamiseks, kuid vaikimisi on sätted väga leebed ja nende muutmine rangemaks on sageli kasutaja jaoks liiga keeruline.

Et selliseid probleeme tulevikus vähendada, on uue Euroopa Liidu isikuandmete kaitse seaduse koostamisel nendele probleemidele mõeldud ja määruse rakendamisel hakatakse andmete vastutavatelt töötlejatelt nõudma tehniliste ja korralduslike

meetmete rakendamist, millega tagataks, et vaikimisi töödeldakse süsteemides ainult neid andmeid, mis on vajalikud töötlemise iga konkreetse eesmärgi saavutamiseks. Kohustus kehtib isikuandmete, nende töötlemise ulatuse, säilitamise tähtaja ja kättesaadavuse osas. Selle nõudega saab tagatud, et isikuandmed ei saa olla vaikimisi kättesaadavad kindlaks määramata isikutele (Euroopa Liidu Teataja L119, 2016).

Praegu kehtivas Euroopa Liidu andmekaitse direktiivis (Euroopa parlamendi ja nõukogu direktiiv 95/46/EÜ, 1995) nimetatakse kuut peamist privaatsuse riivamise viisi:

- *puudulik teavitamine. Inimest, kelle kohta andmeid kogutakse, ei ole sellest teavitatud;*
- *kasutuseesmärgile mittevastamine. Kogutud andmeid kasutatakse lubatust erinevatel eesmärkidel;*
- *nõusoleku puudumine. Isikuandmeid avaldatakse või jagatakse kolmandatele osapooltele ilma isiku nõusolekuta;*
- *turvaaugud ja infolekked. Kogutud andmeid ei käsitleta piisavalt turvaliselt (andmete kuritarvitamine, väärkasutus, vargused, teabe kadumine);*
- *piiratud juurdepääs enda andmetele. Inimesel puudub enda kohta kogutud andmetele juurdepääs ning võimalus ebatäpsusi või väärinfot parandada ja ümber lükata;*
- *andmetöötlejate vastutuse puudumine. Andmetöötlejad ei vastuta nimetatud põhimõtete täitmise eest*.

Enne uute keskkondade kasutuselevõttu peaksid kõik kasutajad üle vaatama keskkonna kasutustingimustest, kas need kuus punkti on kaetud ja vastavalt sellele otsustama, kas seda keskkonda kasutusele võtta ja leppida mõne puudusega või mitte võtta sellist süsteemi kasutusele. Järgnevalt uuritakse millist tüüpi (suletud/avatud) e-keskkondasid e-õppes kasutatakse ja kuidas need oma funktsionaalsuse poolest üldiselt erinevad. Samuti uuritakse milliseid probleeme võib nende keskkondade kasutamisel ette tulla.

2.2 E-õppe keskkonnad

E-õppe keskkond, ehk õpihaldussüsteem, on haridustehnoloogia sõnastikus (kuupäev puudub) toodud definitsiooni järgi elektroonne keskkond õppesisu (nt õppematerjalid, harjutused, testid) ja õppeprotsesside (nt juhendamine, tagasiside, arutelud, kodutööd, rühmatöö, hindamine) haldamiseks.

Tehnoloogilised lahendused (õpihaldussüsteemid, õpiprogrammid, sotsiaalsed tarkvarad jms) on toonud õppeprotsessile hoopis laiaulatuslikuma mõõtme, pakkudes läbi erinevate IKT vahendite lahendusi ja võimalusi õppekeskkonda laiendada ja mitmekesistada (Kusnets, 2007).

Turvalisuse teema on aastatega järjest suurema tähelepanu alla tõusnud. Inglismaal, *Buckinghamshire New University* ülikoolis Bandara, Ioras & Macher (2014) poolt kirjutatud e-õppe küberturvalisuse teemalises dokumendis juhitakse tähelepanu, et e-õppe keskkondades peavad andmed olema kaitstud, et säilitada konfidentsiaalsus, terviklus ja kättesaadavus. Andmete kaitsmine, nendega manipuleerimine, pettused autentimisel ja muud konfidentsiaalsuse küsimused on olulised teemad e-õppes, kuigi samal ajal liigutakse järjest enam suletud keskkondadelt avatud keskkondadele. Praegustes e-õppe keskkondades ei pöörata piisavalt tähelepanu turvanõuetele. Keskkonnad on välja töötatud pedagoogiliste põhimõtete järgi, kuid julgeoleku küsimusi on suures osas ignoreeritud. See võib kaasa tuua soovimatuid olukordi, millel on kahjulik mõju nii õppeprotsessile ja selle juhtimisele kui ka õpilastele ja õpetajatele (Bandara, et al*.,* 2014). Näiteks, kui mõni õpilane tunnetab oma privaatsusele ohtu, kui temalt nõutakse kodutööde esitamist avalikku blogikeskkonda, võib see õpilane muutuda väheaktiivseks, jätta kodutööd esitamata ja saada negatiivse õpikogemuse.

Samadele probleemidele viidatakse ka Nigeeria *Yaba* tehnoloogiakolledžis ja *Babcock* ülikoolis autorite Adetoba B. T., Awodele O. & Kuyoro S.O (2016) kirjutatud artiklis, kus öeldakse, et vähene tähelepanu turvalisuse küsimustele e-õppe keskkondades on probleem, sest kaalul on õpilaste ja õpetajate privaatsus ning ka e-õppe usaldusväärsus. Turvalisuse elementide selgitamisele tuleks rohkem tähelepanu pöörata, et vältida nende rikkumist enne, kui on liiga hilja.

Lorenz, Sousa ja Tomberg (2013) on oma uuringus, mis käsitleb õpilaste teadlikkust

oma privaatsuse õigustest ja selle mõju e-õppes osalemisele, välja toonud, et üldiselt on need õpilased, kes suhtlevad rohkem internetikeskkonas, on ka teadlikumad seal levivatest ohtudest ja seetõttu tunnetavad vajadust kindlama ja turvalisema õppekeskkonna järele. Kuna sotsiaalmeedia keskkonnas õpilased üldjuhul ei filtreeri oma postitusi ega tee vahet, kas nad postitavad sõprade vestlustesse või õppe eesmärgil, võivad nad tunda privaatsuse riivet, kui nendele antav tagasiside on kõigile nähtav. Seetõttu peaks kodutöödele või muudele postitustele antav tagasiside olema privaatne. Õpilastele peab olema tagatud, et nende õppetegevused on potentsiaalsete privaatsuse ohtude eest kaitstud ja õpilane peaks saama e-keskkondades määrata oma informatsioonile (näiteks kodutööd) juurdepääsupiiranguid, et vastavalt keskkonna võimalustele maksimaalselt tagada oma andmete kaitse. Samuti peaks õpetajal olema võimalus anda õpilasele tagasiside privaatselt. Uuringu autorid soovitavad, et vastavad disainimehhanismid tuleks uutesse e-õppele suunatud lahendustesse sisse planeerida ja arendada (Lorenz et al*.,* 2013).

Inglismaa *Bath Spa University* õppejõud Caroline Kuhn´i (2017) uurimus näitab, et paljud õpilased ei tea kuidas orienteeruda internetiavarustes ja veelgi enam, nad kardavad selles avaras keskkonnas ära eksida. Et seda vältida, eelistavad nad pigem püsida oma turvalistes kinnistes õppekeskkondades, mis on neile tuttavad ja õppimine õnnestub paremini (Kuhn, 2017).

Koolides kasutatakse e-õppe keskkonnana nii spetsiaalselt õppetöö haldamiseks loodud õpihaldussüsteeme või ka blogisid või muid sisuhaldussüsteeme (Laanpere, aastaarv puudub).

Üldiselt on spetsiaalselt õppetöö haldamiseks loodud keskkonnad, nt Moodle[3], pigem suletud, mis tähendab, et kursusele ligipääsuks tuleb ennast süsteemi autentida parooli, ID-kaardi või M-IDga ja õpilaste töödele on juurdepääs kas ainult õpetajal või ainult sellel kursusel osalevatel õpilastel. Blogid, vikid ja sotsiaalmeediakeskkonnad, nt Facebook[4], on avatud, mis tähendab, et sealne õppesisu, koos kodutööde ja sellele antud tagasisidega võivad olla nähtavad kõikidele keskkonna kasutajatele. Kuigi ka blogisid ja Facebooki saab kasutada nii, et õppesisu nähtavus oleks piiratud (nt määrata postitustele konkreetsed ligipääsejad või kasutada suletud gruppe). Samuti

3 https://moodle.hitsa.ee/
4 https://www.facebook.com/

saab õppetöös kasutada kombineeritult erinevat tüüpi keskkondi, näiteks tutvuda õpetaja poolt üleslaetud materjalidega suletud keskkonnas, postitada oma arvamuslugu avatud keskkonda, kus teised seda kommenteerida saaksid ja saada õpetajalt tagasiside jälle suletud keskkonda. Või näiteks korraldada avatud keskkonnas kursus, kus saab kasutada näiteks kas videokonverentsi või reaalaja vestlust, et õpilased saaksid omavahel suhelda ja ka õpetajalt küsimusi küsida. Erinevat tüüpi keskkondade positiivsed ja negatiivsed küljed on toodud tabelis 1.

Tabel 1 Avatud ja suletud keskkondade plussid ja miinused

Avatud keskkond		**Suletud keskkond**	
Võimalus	**+/-**	**Võimalus**	**+/-**
Materjalid kiirelt, igal ajal, igast kohast, kõigile kätte-saadavad	+ materjalidele ligipääs kõikjalt, kus on internetiühendus + avalikus keskkonnas postitamine toob kaasa avalikkuse mõju, mistõttu on avaldatavad materjalid kvaliteetsemad ja korrektselt viidatud - tuleb osata vahet teha olulisel ja ebaolulisel infol - oma materjale ja postitusi on kas raske või võimatu eemaldada (digijälg) - me ei tea kes meie materjale ja postitusi loevad	Materjali-de, kätte-saadavad kursuse toimumise ajal, kursusele sisse-logituna	+ ainult kursuse läbimiseks vajalik materjal - pärast kursuse lõppu ei ole materjalid enam kättesaadavad - kuna materjalid on nähtavad ainult piiratud hulgale isikutele, - võidakse viitamata jagada autoriõigusega kaitstud materjale - võidakse jagada autoriõigusega kaitstud materjale ilma omaniku nõusolekuta
Esitatav kodutöö on kõigile nähtav	+ õpilased saavad üksteise töid lugeda ja võivad sellest inspiratsiooni saada - need, kes ei soovi oma mõtteid avalikult esitada, võivad jätta kodutöö esitamata või ei avalda oma kõiki mõtteid - õpilaste selle hetke mõtted on avalikult veebis, mis võib neile soovimatut digijälge tekitada	Esitatav kodutöö on nähtav kas ainult õpetajale või ka kursuse-kaaslastele	+ õpilane saab oma mõtteid vabamalt avaldada, teades, et neid ei näe kõrvalised isikud - puudub võimalus õppida kursusekaaslaste töödest

Keskkond on paljude erinevate võimalus-tega	+ mitmekülgne ja huvitav, ei muutu igavaks + andmeid võimalik üle kanda teistesse süsteemidesse - struktureerimatus, info üleküllus ja liigne funktsionaalsus võib olla väsitav ja häiriv	Keskkond on piiratud funktsio-naalsusega	+ lihtne kasutada oma vähese funktsionaalsuse tõttu - kursuste disain sageli ühesugune ja muutub igavaks - tihti ei ole võimalik e-õppeks vajalike moodulite lisamist (nt test, videokonverents vm) - andmete ülekandmine teistesse süsteemidesse võib olla raskendatud

Lisaks avatusele ja suletusele, on e-õppes kasutatavad keskkonnad ka muu funktsionaalsuse osas erinevad. Näiteks mõned keskenduvad rohkem sellele, et vahendada e-õppe materjale, teised jällegi on rohkem orienteeritud suhtlusele ja tagasisidele. Mõned keskkonnad võimaldavad luua õppesisu ja sellele ligi pääseda ka mobiilsete seadmetega, samas teised seda ei võimalda. Seega peavad õpetajad enne keskkondade kasutuselevõttu kindlaks tegema viisid, kuidas keskkonda kasutada soovitakse, et õppetööd võimalikult tõhusaks muuta. Nad peaksid keskkondade funktsionaalsusi põhjalikult uurima ja arvestama erinevate teguritega, mis keskkonna valimisel võivad olulised olla - näiteks õpilaste vanus, õpetamise ja tagasisidestamise meetod, õpetaja enda kogemus jms (Wright, Lopes, Montgomeria, Reju & Schmoller. 2014).

Kui e-õppe keskkond on selline keskkond, kuhu saab lisada õppematerjale, läbi viia teste ja harjutusi ning anda õpilastele nende kodutöödele või testidele tagasiside (nt Moodle[5], Google Classroom[6]), siis veidi teistsuguse eesmärgiga on õppeinfosüsteemid (nt ÕIS[7], eKool[8]). Õppeinfosüsteemide olulisimaks osaks on tunniplaani ja klassipäeviku funktsionaalsus. Seal hallatakse ka puudumistõendeid, märkuseid ja kiituseid. Seega on see pigem administratiivne vahend kooli ja kodu vahelises suhtluses, kui õppetöö keskkond. Neist kahest erinevad omakorda keskkonnad, mis võimaldavad peamiselt õppematerjalide vaatamist, üleslaadimist või ühistööd

5 https://moodle.com/
6 https://classroom.google.com/u/0/h
7 http://ois.tlu.ee/pls/portal/ois2.ois_public.main
8 https://ee.ekool.eu/index_et.html

dokumentidega (nt Google drive[9], Miksike[10]). Neljandaks erinevaks tüübiks on e-õpet toetavad rakendused. Selliseid rakendusi on väga palju, näiteks erinevad testide läbiviimise keskkonnad või konkreetse aine õppimiseks loodud rakendused (nt Kahoot[11], 10 Monkeys[12]). Veel ühe tüübina on e-õppes kasutusel sotsiaalmeedia- ja blogikeskkonnad (nt Facebook[13], Wordpress[14]). Kõiki neid erinevat tüüpi keskkondasid saab e-õppes kas eraldiseivatena või ühildatuna kasutada.

Samas leiab Siemens (2004), et kahjuks valitakse sageli e-õppe läbiviimiseks valedel eesmärkidel valed keskkonnad, mis toob endaga kaasa negatiivse õpikogemuse, õppe ebaefektiivsuse ja nii rahalised kui ajalised asjatud kulutused.

Samuti võib negatiivne kogemus tekkida, kui kasutatavaid keskkondasid on liiga palju. Üldiselt eeldavad enamus keskkondi kasutajakonto loomist. Vähestesse keskkondadesse saab sisse logida kas Id-kaardi või m-IDga. See tähendab, et luua tuleb mitmeid kasutajakontosid erinevate paroolidega. Erinevatel keskkondadel on parooli nõuded erinevad, nii saab mõnesse keskkonda luua ainult tähtedest koosneva parooli, mõnes keskkonnas tuleb tähtedele lisada ka numbreid ja muid sümboleid, nõutud on ka erinevate tähemärgipikkustega paroolid. Kasutajatel on lõpuks väga raske kõikide keskkondade paroole meeles pidada, neid hakatakse kas kuhugi üles kirjutama või kasutama erinevates keskkondades samu paroole. Või paroolid lihtsalt ununevad ja kui neid uuendada ei osata või ei ole see tehniliselt võimalik, siis luuakse keskkondadesse topelt kontosid, mis suurendab kasutajate digijälge. Sarnastest paroolidega seonduvatest probleemidest räägib ka USA Tarbijakaitse Ameti tehnoloog Lorrie Cranon (2016) oma uurimuses „*Time to rethink mandatory password changes*“.

Magistritöö esimesest peatükist selgus, et digipädevuste nõuetes on nii õpetajatele kui õpilastele kirjeldatud ootused. Õpilastelt oodatakse, et nad tunneksid digikeskonna ohtusid ning oskaksid kaitsta oma identiteeti, isikuandmeid ja privaatsust (vt pt 1.1) ja õpetajatelt, et nad oskaksid soovitada õpilastele turvalisi keskkondi ja juhendada neid turvateadlikult kasutama (vt pt 1.2). Teisest peatükist selgus, et keskkondi, mida

9 https://drive.google.com
10 http://www.miksike.ee
11 https://getkahoot.com/
12 https://www.10monkeys.com/ee/
13 https://www.facebook.com/
14 https://wordpress.com

e-õppes kasutada saab, on palju erinevaid. Neil on erinev funktsionaalsus ja omad positiivsed ja negatiivsed küljed (vt pt 2.2). Samuti selgus, et kui nende erisustega ei arvestata või kui enne keskkonna kasutuselevõttu ei tutvuta selle kasutustingimustega ega muudeta turvasätteid rangemaks, võib kannatada saada nii turvalisus, privaatsus kui ka õpikogemus üldiselt (vt pt 2.1).

Eeltoodust lähtuvalt on empiirilise uurimuse lähtekohtadeks:

- õpilaste, õpetajate ja haridustehnoloogide hinnangud enese teadlikkusele turvalisuse valdkonnas;
- õpilaste, õpetajate ja haridustehnoloogide üldised harjumused turvakäitumisel – nt kontode loomine ja turvalisuse- ja privaatsussätetega tutvumine;
- millistes küsimustes vajavad õpilased, õpetajad ja haridustehnoloogid abi teistelt;
- milliseid e-keskkondi Eesti koolides kasutatakse;
- kas e-keskkondade kasutamist peetakse oprimaalseks;
- kas e-keskkondade kasutamisel on esinenud mingeid turvalisuse või privaatsuse probleeme.

Töö teoreetiline osa annab sisendi empiirilise uurimuse läbiviimiseks. Uurimuse läbiviimise metoodikat kirjeldatakse peatükis 4 ja uurimise tulemused võetakse kokku peatükis 5.

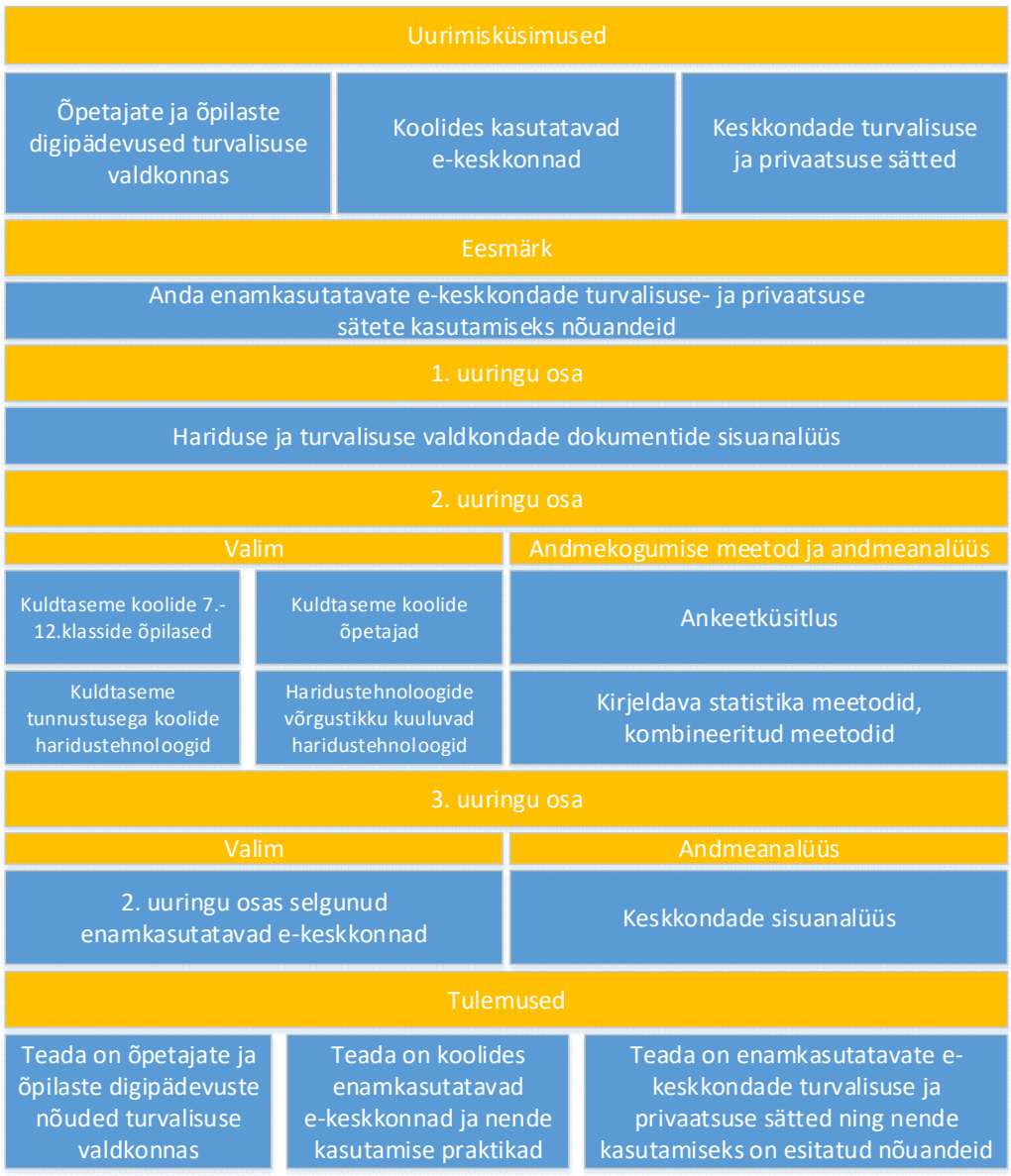
3 Uurimistöö metoodika ja valim

Töö teoreetiline osa (pt 1 ja 2) käsitles endas õpilastele ja õpetajatele esitatavate nõuete analüüsi. Uuriti väljatöötatud ja kehtivaid nii riiklikke kui välismaiseid strateegiaid, õppekavasid, digipädevuste mudeleid ja erinevaid programme ning seda kõike just turvalisuse ja privaatsuse vaatenurgast. Lisaks nõuete analüüsile uuriti ka erinevate e-keskkondade olemust, milles õpilased ja õpetajad tegutsevad ning toodi välja nii avatud kui suletud keskkondade head ja vead.

Töö empiiriline osa koosneb kahest osast. Esimeses osas selgitatakse milliseid ja mis tüüpi e-keskkondasid Eesti koolides kasutatakse ja milliseid probleeme on nende kasutamisel turvalisuse ja privaatsuse valdkonnas ette tulnud. Uuritakse millised on levinud kontode loomise praktikad ja millistel teemadel vajavad nii õpilased kui ka õpetajad ja haridustehnoloogid kõige enam abi ja informatsiooni.

Uurimuse teine osa käsitleb esimesest osast selgunud enamkasutatavate e-keskkondade turvalisuse ja privaatsuse sätete analüüsi. Uuritakse viie enamkasutatava e-keskkonna sätteid ja analüüsitakse, kas nende keskkondade kasutustingimustes on käsitletud Euroopa Liidu andmekaitse direktiivis (1995) nimetatud levinumaid privaatsuse eiramise viise. Lisaks tuuakse välja nende keskkondade turvalisuse ja privaatsuse sätted koos nõuannetega, kuidas neid sätteid oleks turvalisust ja privaatsuse kaitset silmas pidades otstarbekas kasutada. Soovitusi saab kasutada näiteks õpilastega koos nende sätete ülevaatamiseks ja arutamiseks, miks üht või teist sätet just nii kasutada võiks.

Et anda ülevaade magistritöö valmimise protsessist tervikuna, kujutatakse alljärgnevalt skemaatiliselt uurimuse läbiviimise protsessi (Joonis 2). Joonis annab üldise ülevaate uurimisküsimustest, uurimuse eesmärgist, erinevate uuringu osade valimist, andmekogumise meetoditest ja andmeanalüüsi meetoditest. Samuti annab joonis kokkuvõtva ülevaate uurimistulemustest.



Joonis 2 Uuringu protsessiskeem

Detailsemalt kirjeldatakse valimi moodustamist, erinevate uuringuetappide, andmekogumise meetodeid ja andmeanalüüsi meetodeid alljärgnevates peatükkides.

3.1 Ankeetküsitlus

Andmekogumise meetodiks valis autor küsitlusankeedi, mis on toodud ära ka lisas 2. Küsitlusankeedi kasuks otsustas autor põhjusel, et soovis saada võimalikult laia ülevaadet, ning küsitleda selleks paljusid erinevaid koole, haridustehnolooge, õpetajaid ja õpilasi. Ankeet vormistati Google forms keskkonnas, neljale erinevale

rollile – haridustehnoloog (või tema ülesandeid täitev isik), õpetaja, õpilane ja koolijuht. Enne küsimustikule vastamist pidi vastaja valima rolli. Rollidel mõned küsimused kattusid ja mõned küsimused erinesid (vt Lisa 2). Küsimused olid jaotatud kolme alamteema alla: üldine e-õppe kasutus, turvateadlikkus ja suhtumine ning toe vajadus. Uurimust ei saa pidada puhtalt kvantitatiivseks uurimuseks, kuna ankeet sisaldas lisaks valikvastustega küsimustele ka avatud vastustega küsimusi. Ühes uurimuses kvantitatiivsete ja kvalitatiivsete meetodite kasutamist toetavad ka uurijad Ghauri ja Gronhaug (2014).

Valim moodustati eesmärgistatud valimi põhimõttel, lähtudes uurimisküsimustest. Eesmärk oli, et küsimustikule vastaksid eelkõige digitaalselt aktiivsed koolid, kellel juba on e-keskkondade kasutamisel mõningane kogemus. Seega valiti esmalt välja 2016. aastal HITSAlt[15] digitaalselt aktiivse kooli kuldtaseme tunnustuse pälvinud koolid. Kuna neid koole oli kokku 27 tk, millest enamus olid ainult põhikoolid (kuid uurida sooviti ka gümnaasiumi osa), kitsendati valimit nii, et sinna jääksid sellised kuldtaseme koolid, kellel on koosseisus nii põhikool kui ka gümnaasium. Nendes kooliastmetes peaksid õpilased omama juba mõningaid digipädevusi selles osas, kuidas e-keskkondi turvaliselt kasutada ja kuidas oma andmeid ja identiteeti e-keskkondades kaitsta. Nii jäi lõplikusse valimisse 8 kooli: Gustav Adolfi Gümnaasium, Tallinna Reaalkool, Pelgulinna Gümnaasium, Kohtla-Järve Gümnaasium, Kuressaare Gümnaasium, Tabasalu Ühisgümnaasium, Tartu Kesklinna kool ja Tallinna Lilleküla Gümnaasium.

Enne küsimustiku väljasaatmist vastas küsimustikule väike rühm haridustehnolooge, kelle nõuannete järgi ankeeti kohendati. Lõplik ankeet saadeti välja valitud koolide haridustehnoloogidele palvega täita küsitlus ise ja edastada see ka oma kooli õpetajaskonnale ning 7. - 12. klasside õpilastele. Ankeet saadeti välja 15. veebruaril 2017. aastal. Kui ankeet oli välja saadetud, helistas autor kõik valimisse võetud koolide haridustehnoloogid isiklikult läbi, et veenduda ankeedi kohale jõudmises. Autor selgitas adressaatidele töö põhimõtteid ja eesmärke ning palus ankeedi edastada 7. - 12. klasside õpilastele ja õpetajatele ning täita ankeet ka ise. Kuldtaseme koolidele võrdluse saamiseks saatis autor ankeedi välja ka haridustehnoloogide listi haridustehnoloogid@lists.eenet.ee. Ankeet oli vastamiseks avatud 15. veebruarist

15 http://www.hitsa.ee/ikt-hariduses/digitaalselt-aktiivne-kool/kuldtase

kuni 10. märtsini 2017. aastal. 10. märtsi õhtuks oli küsimustikule vastatud 507 korral. Vastajate hulgas oli 227 põhikooli (7. - 9. klass) õpilast, 203 gümnaasiumi (10. - 12. klass) õpilast, 58 õpetajat, 18 haridustehnoloogi ja 1 koolijuht.

Sellise andmete kogumise meetodi eeliseks oli see, et võimalik oli koguda palju andmeid paljudelt erinevatelt isikutelt. Sellise kogumisviisi miinuseks on aga see, et autor oli täielikus sõltuvuses sellest, kas haridustehnoloog saadab ankeedi edasi ka õpetajaskonnale ja õpilastele või mitte. Samale nõrkusele andmete kogumisel viitasid ka Ghauri ja Gronhaug (2004). Koostööst keeldumiste põhjustena toovad Ghauri ja Gronhaug (2004) välja selle, et inimestel võib olla aja- ja motivatsioonipuudus, kui ka kardetakse negatiivseid tagajärgi, kui ollakse siiras oma vastustes. Sarnased põhjused selgusid ka telefonivestlustest haridustehnoloogidega, kus põhjendati ankeedi enda käes hoidmist ja mitte edasi saatmist sellega, et kevadel laekub koolidesse palju ankeete väljastpoolt maja, millele vastata. Lisaks viivad gümnaasiumite üheteistkümnendad klassid samaaegselt läbi oma uurimusi. Suurimaks põhjuseks peeti SA Innove [16]poolt samal ajal üldhariduskoolides korraldatavat riiklikku rahuloluküsitlust, mis hõlmab kõiki Eesti kaheksanda ja üheteistkümnenda klassi õpilasi, lapsevanemaid ja üldhariduskoolide õpetajaid. Paljud ütlesid, et ise täidavad ankeedi kindlasti, kuid õpetajatele ja õpilastele peale käima ei hakka. Ankeedi link lubati lisada küll oma kooli veebilehele või e-õppe keskkonda, kuid enamat teha ei julgeta, kartes õpetajaskonna pahameelt kuni võimaliku suhete rikkumiseni. Mõni kool muretses ka selle pärast, et töö tulemusena hakatakse koole võrdlema ja uurimusest tulevad välja mõne kooli kitsaskohad. Sellest viimasest hirmust tulenevalt kinnitas autor kõikidele ankeedi saajatele, et ankeedis küsitakse vaid kooli nime üldiseks infoks, et autorile oleks teada, millistest koolidest vastati, kuid sisulist võrdlust vastuste vahel ei tehta ega tooda ka konkreetsete vastuste juures välja millisest koolist kuidas vastati.

Enne andmete analüüsi kontrolliti ja viimistleti andmed. Eemaldati ainus koolijuhi ankeet, sest üksikuna ei võimalda see koolijuhtide seas üldiseid järeldusi teha. Võimalikult laia pildi saamiseks kasutati uurimuses kombineeritult kvantitatiivseid ja kvalitatiivseid meetodeid (Hisjärvi, Remes & Sajavaara, 2010). Andmeanalüüsi meetodina kasutati valikvastustega küsimuste puhul kirjeldava statistika meetodeid,

[16] https://www.innove.ee/et/uudised/728/algasid-ulatuslikud-haridusega-rahulolu-kusitlused

tuues töö tulemustes välja erinevate rollide vastused summaarselt. Avatud vastustega küsimusi analüüsiti, kodeeriti vastavalt uurimisprobleemidele märksõnadega ja tõlgendati. Vastuste vahel otsiti ühiseid jooni ja erinevusi (Ghauri & Gronhaug, 2004). Tulemused esitatakse töös grupeeritult osaliselt tabeli kujul ja osaliselt kirjeldava tekstina.

3.2 E-keskkondade turvasätete analüüs

Ankeetküsitlusega selgitatati milliseid e-keskkondasid Eesti koolides kõige enam kasutatakse ning kas ja milliseid probleeme nende kasutusel esineb. Enamkasutatavad keskkonnad jaotati vastavalt peatükis 2.2 väljatoodud funktsionaalsuse erinevustele viide kategooriasse – e-õppe keskkonnad, õppeinfosüsteemid, keskkonnad mida saab kohandada e-õppeks (nt sotsiaalmeedia keskkonnad, vikid ja blogid), e-õpet toetavad rakendused ja veebikeskkonnad õppematerjalide lisamiseks, kasutamiseks ja ühistöö tegemiseks. Pärast kategooriatesse jagamist valiti igast kategooriast keskkond, mida nimetati uuringus kõige rohkem. Sellisteks keskkondadeks olid Moodle, eKool, Facebook, Kahoot ja Google drive. Autor analüüsis kasutustingimusi ning turvalisuse ja privaatsuse sätteid ning katsetas võimalusel sätted praktiliselt läbi. Autor võttis ühendust ka eKooli arendajaga ning uuris, kas töös oleks võimalik kirjeldada ka administraatori tasandi sätteid, kuid neid autorile siiski ei avaldatud. Ka Moodle puhul võttis autor ühendust HITSA Moodle halduriga, kes võimaldas analüüsis välja tuua ka Moodle administraatori sätted. Kuna Moodlet võib iga kool hallata ka ise (ei pea kasutama HITSA poolt pakutavad Moodlet), on töös analüüsitud ka administraatori sätteid.

Töö tulemusena koostati koondtabel levinumatest privaatsuse eiramine viisidest keskkondade kasutuslepingutes ja märgiti, kas käesoleva magistritöö uurimisobjektideks olevate keskkondade kasutustingimustes sarnaseid probleeme esineb (Tabel 5). Lisaks loetleti nende keskkondade turvalisuse ja privaatsuse sätted, toodi välja vaikesäte ning anti soovitusi kas, miks ja kuidas vaikesätet võiks muuta (Lisa 1).

4 Ankeetküsitluse tulemused

Neljandas peatükis antakse ülevaade ankeetküsitlusega selgunud tulemustest. Tulemused esitatakse ankeedis esinenud teemade kaupa: valmis olnud koolide üldine e-õppe kasutuse taust, kasutajate turvateadlikkus ja suhtumine ning nõustamise vajadus.

4.1 Üldine e-õppe kasutus

Ankeetküsitluse esimene osa uuris üldist e-õppe kasutust uuringus osalenud koolides. Vastajatelt uuriti kuidas nad hindavad praegu nende koolis kasutatavate e-keskkondade mahtu, mis tüüpi keskkondasid nad eelistavad kasutada (suletud/avatud/kombineeritud), milliseid keskkondi nad üldse kasutavad ning kui palju kasutatakse õppetöös sotsiaalmeedia keskkonda, näiteks Facebooki.

Hetkel koolis kasutatavate e-keskkondade mahu kaardistamise eesmärk oli teada saada kas digitaalselt aktiivsetes koolides on e-õppe maht juba saavutanud mingi taseme, kus õpilased ja õpetajad tunnevad, et seda on juba liiga palju või hinnatakse mahtu väheseks, mis tähendab, et e-keskkondade kasutamine jätkub tõusvas joones.

Küsimusele „Kuidas hindad e-keskkondade kasutuse mahtu teie koolis?“, vastati igas rollis (õpilased 59,5%, õpetajad 74,1%, haridustehnoloogid 66,7%) kõige enam, et mahtu peetakse optimaalseks, kuid trend näitab pigem ootust enamale kui vähemale e-keskkondade kasutusele, pidades praegust olukorda kas väheseks või pigem väheseks (õpilased 31,6%, õpetajad 15,5%, haridustehnoloogid 33,3%). Antud trend näitab, et kui isegi digitaalselt aktiivsed koolid tunnetavad veel pigem vähest e-keskkondade kasutust, siis on tõenäoline, et e-keskkondade kasutuse maht suureneb neis kooldes veelgi ja kindlasti suureneb see vaikselt ka digitaalselt madalama aktiivsusega koolides. Mis omakorda tähendab, et e-keskkondade turvalisuse ja privaatsuse olulisus ja mure selle pärast ei ole vähenemas, vaid seda tuleb jätkuvalt fookuses hoida ja paralleelselt koos keskkondade kasutuselevõtuga tutvustada õpilastele ka turvalisuse ja privaatsusega seonduvaid võimalusi ja esineda võivaid probleeme.

Järgmiseks sooviti välja selgitada millist tüüpi e-keskkondasid kasutada eelistatakse. Kas pigem eelistatakse kasutada suletud keskkondi, mis viitaks suuremale privaatsuse vajadusele või hoopis blogilaadseid avatud keskkondi, kus nii õppematerjalid kui õpilaste tööd ja sageli ka õppetulemused on avalikult kõigile kättesaadavad.

Küsimusele "Kas koolis kasutatavad e-keskkonnad võiksid sinu arvates olla?", vastati järgmiselt:

Tabel 2 Eelistatud e-keskkonna tüüp

Valikvastus	**Õpilane**	**Õpetaja**	**HT**
Avatud (kõik, kes keskkonda sisenevad, saavad lugeda ülesandeid ja tehtud töid)	35 (8,1%)	1 (1,7%)	1 (5,6%)
Suletud, kuid avatud grupile (keskkonda saab siseneda parooliga ja sisestatud infot näevad vaid grupi liikmed).	**161 (37,4%)**	14 (24,1%)	7 (38,9%)
Sh kinnine (keskkond võimaldab teha ülesandeid nii, et vastuseid näeb ainult õpetaja)	**79 (18,4%)**	2 (3,4%)	-
Kombineeritud (vastavalt vajadusele)	155 (36,1%)	**41 (70,7%)**	**10 (55,6%)**

*HT-haridustehnoloog või tema ülesandeid täitev isik

Õpilaste hulgas leiti kõige enam (55,8%), et nad eelistaksid kasutada keskkondi, mis on kas suletud (kuid avatud grupile) või täiesti suletud (tööd nähtavad ainult õpetajatele). Õpetajad ja haridustehnoloogid (vastavalt 70,7% ja 55,6%) eelistavad kasutada kombineeritud keskkondasid vastavalt vajadusele. Järgmiseks valikuks on ka õpetajate ja haridustehnoloogide seas suletud keskkonnad (vastavalt 24,1 % ja 38,9%). Täielikult avatud keskkondades õpet ei peeta üheski rollis eelistatuks. Kuigi teooria viitab (Bandara et al., 2014) sellele, et pigem liigutakse tulevikus e-õppes rohkem avatud keskkondade kasutamisele, nähtub siinsetest vastustest, et pigem eelistatakse suletud keskkondasid või vajadusele vastavalt kombineeritud keskkondasid.

Edasi uuriti milliseid e-keskkondasid koolides üldse kasutatakse. Küsimuse eesmärgiks oli teada saada milliseid keskkondi üldse kasutatakse ning kas keskkonna tüübi eelistus kajastub kuidagi ka keskkondade kasutuses.

Avatud vastusega küsimuse “Milliseid e-keskkondasid kasutatakse teie koolis?”, all nimetati kokku 160 erinevat nimetust. Keskkonnad jaotati vastavalt nende tüübile, funktsioonile ja võimalustele viide gruppi. Allolevas tabelis 3 esitatakse tulemused, mida nimetati üle 10 korra. Sulgudes on märgitud kordade arv, mitu korda keskkonda ankeedis nimetati.

Tabel 3 Enamkasutavad e-keskkonnad

E-õppe keskkond	Õppe-infosüsteem	Keskkond, mida saab kohandada e-õppeks	E-õpet toetav rakendus	Veebikeskkond õppematerjalide lisamiseks ja kasutamiseks
Moodle (203) Google classroom (22) Õpiveeb (21) Foxcademy (15)	**eKool (99)** Stuudium (11)	**Facebook (116)** Blogi-keskkonna (35)	**Kahoot (178)** Quizlet (96) Socrative (31) Quizizz (29) Endomondo (13)	**Google drive (358)** Miksike (55) Youtube (24) Nutisport (21) Padlet (19) Learningapps (16) Geogebra (13)

Kuna teooria viitas, et suundumus on pigem avatud keskkondadele ja Facebook on üks nendest avatud keskkondadest, mida palju kasutatakse, uuriti ka seda, kui palju sotsiaalmeediat õppetöös kasutatakse. Vastanud õpilastest 74% tarbivad Facebooki õppetöös vähemalt kord kuus. Õpetajad ja haridustehnoloogid väidavad ennast Facebooki õppetöö osana kasutamas vähemalt kord kuus vastavalt 44,8% ja 83,3%. Ülejäänud vastajad õpetöös Facebooki ei kasuta või kasutavad harvemini kui kord kuus.

4.2 Turvateadlikkus ja suhtumine

Teadlikkuse ja suhtumise küsimuste plokis uuriti kui teadlikuks vastajad ennast turvaprobleemide osas peavad, kui oluliseks nad peavad keskkondade turvalisuse ja privaatsuse sätteid ning kas nad tutvuvad nende sätetega enne uute keskkondade kasutuselevõttu. Ning ka seda, kas e-keskkondade kasutusel on neil esinenud mingeid turvalisuse või privaatsuse probleeme. Eesmärgiks oli uurida kuidas on kasutajate

üldine suhtumine turvalisuse sätetesse ja kui ka sellest uuringust selgub sama, mis selgus teooria uurimisel, et tegelikult turvasätetega ei tutvuta (vt pt 2.1), siis mis on need põhjused miks sätetega ei tutvuta.

Tabel 4 Turvateadlikkus ja suhtumine

Valikvastus	**Olen teadlik erinevatest ohtudest mis võivad e-keskkondasid kasutades, turvalisuse ja privaatsuse sätteid eirates, ette tulla**	**Nõustun väitega, et keskkondade turvalisuse ja privaatsuse sätted on olulised**	**Tutvun enne uue keskkonna kasutuselevõttu selle turvalisuse ja privaatsuse sätetega**
Õpilane			
Ei	20 (4,7%)	9 (2,1%)	79 (18,4%)
Pigem ei	29 (6,7%)	11 (2,6%)	**88 (20,5%)**
Nii ja naa	**132 (30,7%)**	68 (15,8)	**164 (38,2%)**
Pigem jah	**153 (35,6%)**	**90 (20,9%)**	74 (17,2%)
Jah	96 (22,3%)	**252 (58,6%)**	25 (5,8%)
Õpetaja			
Ei	2 (3,4%)	-	7 (12,1%)
Pigem ei	6 (10,3%)	-	11 (19%)
Nii ja naa	**19 (32,8%)**	5 (8,6%)	**14 (24,1%)**
Pigem jah	**25 (43,1%)**	**14 (24,1%)**	**16 (27,6%)**
Jah	6 (10,3%)	**39 (67,2%)**	10 (17,2%)
Haridustehnoloog			
Ei	1 (5,6%)	-	-
Pigem ei	1 (5,6%)	1 (5,6%)	1 (5,6%)
Nii ja naa	1 (5,6%)	1 (5,6%)	2 (11,1%)
Pigem jah	**11 (61,1%)**	**4 (22,2%)**	**12 (66,7%)**
Jah	**4 (22,2%)**	**12 (66,7%)**	**3 (16,7%)**

Ohtudest teadlikkuse osas vastati igas rollis kõige enam (õpilane 35,6%, õpetaja 43,1%, haridustehnoloog 61,1%), et ohtudest ollakse pigem teadlikud. Kui õpilaste ja õpetajate puhul näitab trend teadlikkuse langevust, siis haridustehnoloogide puhul on trend tõusev.

Väite osas, kas ollakse nõus, et turvasätetega tutvumine on oluline, vastati igas rollis sarnaselt – kõige enam vastati „Jah“, ning järgmiseks „Pigem jah“.

Küsimuses, kas sätetega tutvutakse või mitte, esineb rollide vahel kõige rohkem erinevusi. Enamus õpilasi (38,2%) vastavad, et tutvuvad sätetega „Nii ja naa“. Õpetajad (27,6%) ja haridustehnoloogid (66,7%) vastavad, et pigem tutvuvad sätetega. Õpilaste ja õpetajate puhul on trend langev – järgmine hulk õpilasi (20,5%) ütleb, et nad pigem ei tutvu sätetega ja õpetajad (24,1%) tutvuvad „Nii ja naa“. Haridustehnoloogide puhul on trend tõusev, 16,7% vastab, et tutvub sätetega kindlasti.

Kui küsimusele „Kas tutvute tavaliselt enne uue keskkonna kasutuselevõttu selle turvalisuse ja privaatsuse sätetega?“ vastati “Ei” või “Pigem ei”, paluti vastanutel välja tuua põhjused, miks nad sätetega ei tutvu.

Õpilaste hulgas toodi kõige sagedamini (136 korral) põhjuseks seda, et sätted on tavaliselt liiga pikad ja keerulised. Õpetajate poolt kõige enam (16 korda) nimetatud põhjus oli see, et kui nii paljud seda keskkonda kasutavad, siis ei saa siin neile midagi mittesobivat olla. Haridustehnoloogid nimetasid kahel korral põhjuseks seda, et kuna keskkonna võtab kasutusele õpetaja, peab ka tema ise selle sätetega tutvuma.

Vastustest nähtub, et kuigi turvalisust peetakse oluliseks, ei tutvuta siiski keskkondade sätetega. See näitab, et kuigi keskkonnad pakuvad erinevaid võimalusi, arvavad kasutajad, et need on vaikimisi keskkonna halduri poolt piisavalt turvaliseks seatud ja et nemad selle pärast enam muretsema ei pea. Kuna haridustehnoloogid ise pigem loevad või loevad kindlasti turvalisuse sätteid, eeldavad nad ka õpetajatelt, et nad seda teeksid, mitte ei usaldaks pimesi teiste valikuid.

Samas küsimuste plokis uuriti veel ka seda, kas kasutuselolevates keskkondades on neil ette tulnud turvalisuse- ja privaatsuse probleeme. Küsimustele “Kas mõne keskkonna kasutamisel on sul esinenud mingeid turva- või privaatsusprobleeme?” ja “Kui vastasid “Jah”, siis palun nimeta keskkond ja kirjelda probleemi”, vastati

jaatavalt koos kommentaariga üheksateistkümnel korral. Vastused kodeeriti turvalisuse kolme põhikomponendi alusel käideldavuse, tervikluse ja konfidentsiaalsuse probleemideks ja sellest nähtus, et teistest probleemidest enam toodi välja käideldavuse probleeme, kus näiteks kas oldi unustatud paroolid või oli keskkond muutunud tasuliseks ja materjalid ei olnud enam kättesaadavad või oli kasutajakonto kaaperdatud. Vastustest paistis silma ka see, et enamus probleeme oli seotud sotsiaalmeedia keskkonnaga Facebook, mistõttu võetakse selle keskkonna turvalisuse ja privaatsuse sätted ka selles töös analüüsimisele.

4.3 Toe vajadus

Siinses peatükis uuriti kasutatavaid praktikaid ja küsimusi, mis osas vastajad tuge ootavad – kas keskkondadesse kontode loomisel, nende haldamisel, keskkondade kasutamisel või muus.

Esmalt uuriti kontode loomise praktikaid selles osas, kas tavaliselt loovad keskkondadesse omale kontod õpilased iseseisvalt, luuakse need õpetaja juhendamisel koolis kontakttunnis või loob õpilastele konto õpetaja. Kõikide rollide vastustest nähtus, et üldiselt luuakse uude keskkonda konto õpetaja juhendamisel kontakttunnis, kuid, et vahel harva peavad õpilased konto loomisega ka iseseisvalt hakkama saama. Kuna üldiselt õpetajate poolt õpilastele kontode loomist ei toimu, tähendab, et õpetajate vastutus võõraste kontode paroolide haldamise on pigem maandatud.

Küsimusele „Millist abi oled vajanud ja saanud e-keskkondade kasutamisel koolist?“, vastas 41,6% õpilastest, et on abi otsinud ja ka abi saanud parooli ununemisel, 32,6% õpilastest vajas ja sai ka abi konto loomisel ja 29,5% õpilastest vajas abi erinevate keskkondade kasutamisel. Nimetati ka keskkonna turvasätete muutmist, keskkondade avatuse ja suletuse teemasid, internetis turvaliselt käitumist ja konto sulgemist.

Uuriti ka seda, kas mõnes küsimused on nad jäänud abita. Küsimusele „Kui oled jäänud mõnes küsimuses abita, siis millises küsimuses?“, toodi välja järgmiseid lahendamata küsimusi:

- kuidas Facebooki kontot kustutada;
- kuidas mingi pisiasi mu tööd efektiivsemaks teeks;
- kuidas probleemi lahendada kui nt midagi „kinni kiilub“;

- kuidas ma saan kindel olla, et mu töö on salvestatud ja ma pääsen sellele ligi;
- mida teha kui keegi teeb minu nime alt midagi, mida ma ei saa takistada isegi siis, kui olen paroolid vahetanud, kuhu sel juhul pöörduda;
- miks kool kasutab vananenud ja ebaturvalist Moodlet;
- kuidas muuta privaatsuse sätteid keskkonnas nii, et liigne avalikkus mulle kahju ei teeks (digijälge ei tekitaks);
- kuidas sulgeda konto kui ma seda enam ei vaja;
- ühest keskkonnast ei osanud välja logida.

Sama uuriti ka õpetajatelt ja haridustehnoloogidelt, et kas ja millistes küsimustes on õpilased nende poole pöördunud, kuid nad on jäänud vastamisel hätta. Vastustest nähtus, et õpetajad on jäänud kõige enam hätta parooli vahetuse teemadel, kui õpilane on parooli unustanud. Keskkondade kasutamise nõustamisel on hätta jäänud nii õpetajad kui haridustehnoloogid. Nimetatakse ka konto loomist mõnda keskkonda, keskkondade avatuse ja suletuse teemasid ning konto sulgemist. Haridustehnoloogid tõid välja ka rohkem IT-valdkonda kuuluvaid küsimusi (nt halb interneti levi).

Kui õpetajad on õpilaste küsimustele jäänud vastused võlgu, uuriti, kelle juurde nad õpilase suunavad või kellelt ise abi küsivad, et õpilasele vastata. Küsimusele „Kellelt te e-keskkondadega tekkivate küsimuste puhul abi saate või kelle poole suunate õpilase, kui te ise ei oska teda aidata?“, nimetati kõige enam – 77,6%, oma kooli IT-juhti või teist IT-töötajat. Mõned protsendid vähem – 74,1%, saadi abi oma kooli haridustehnoloogilt või tema ülesandeid täitvalt isikult ja 41,4% õpetajaid nimetas oma kooli teist kolleegi.

Toe vajaduse küsimuste vastusets nähtub, et kõige enam on õpilased vajanud ja saanud abi ununenud parooli vahetusega (41,6%). Sama toetavad ka õpetajate ja haridustehnoloogide vastused, kus 53,4% õpetajatest ja 77,8% haridustehnoloogidest ütlevad, et õpilased on kõige enam pöördunud nende poole ununenud parooli taastamise sooviga. Samas tunnistavad nii õpetajad kui haridustehnoloogid, et nad on samas küsimuses jäänud õpilaste abistamisel hätta ja on pidanud abi otsima kelleltki teiselt. Turvalisuse osas pigem nõu ei küsita, samas näitavad õpilaste vastused, et hätta on enamus juhtudel (8 vastanust 6) jäädud just turvalisuse teemadega – konto kustutamine ja sulgemine, keskkonnast väljalogimine, andmete avalikkus, privaatsus, andmetele ligipääsemine, ebaturvalise keskkonna kasutamine. Üldiselt näitab see

seda, et õpilastel tekib e-keskkondade kasutamisel erinevaid probleeme, nad ka pöörduvad õpetaja või haridustehnoloogi poole, kuid ka nemad alati ei oska õpilast aidata ja peavad probleemide lahendamiseks edasi pöörduma.

Viimaseks uuriti millistel teemadel üldiselt tuntakse vajadust nõustamise järele ja selgus, et kõikides rollides (54% õpilasi, 55,2% õpetajaid ja 72,2% haridustehnolooge) vajatakse kõige enam infot nende turvalisuse ja privaatsuse probleemide kohta, mis tekitavad neile soovimatut digijälge, kuid oluliseks peeti ka nõustamise saamist keskkondade turvalisuse ja privaatsuse sätete kasutamisel ja nende kasutamisel tekkinud probleemide lahendamisel.

Kuna antud magistritöö teemaks on e-keskkondade turvalisus ja privaatsus, siis uuritakse selle töö kontekstis edasi ankeedis nimetatud ja autori poolt viide erinevasse kategooriasse jaotatud keskkondadest kõige enam väljatoodud keskkondade turvalisuse- ja privaatsuse sätteid.

5. E-keskkondade turvalisuse ja privaatsuse sätete ülevaade ja soovitused

Enamkasutatavad keskkonnad, mis selgusid empiirilisest uurimusest, on Moodle, eKool, Facebook, Kahoot ja Google drive. Järgnevalt uuritakse nende keskkondade võimalusi, koostatakse nende kohta ülevaatlik infotabel, analüüsides nende keskkondade kasutustingimusi Euroopa Liidu andmekaitse direktiivis (1995) nimetatud privaatsuse riivamise võimaluste valguses, hinnates, kas need punktid on keskkondade kasutustingimustes välja toodud (Tabel 5). Lisaks koostatakse turvalisuse ja privaatsuse sätete ülevaade (Lisa 1), milles tuuakse välja keskkonna turvalisuse ja privaatsuse sätted, vaikesätted ja soovitused nende sätete muutmiseks.

5.1 Moodle

Moodlet nimetati vastustes 203 korral, mis on ülekaalukalt teistest nimetatud e-õppe keskkondadest üle. Moodle[17] on suletud e-õppe keskkond, mis nõuab autentimiseks kasutajanime ja parooli. Sisse saab logida ka ID-kaardi ja M-IDga. Moodlet saab seadistada nii, et õpilase poolt sisestatut näeb kas ainult õpetaja või ka samasse gruppi kuuluvad õpilased.

Moodle[18] võimaldab luua nii 100% e-õppe kursuseid kui ka osaliselt e-õppe ja osaliselt kontaktõppe kursuseid. Moodle arendamise protsessis pööratakse suurt tähelepanu andmete turvalisusele ja kasutajate privaatsusele. Turvalisust arendatakse pidevalt, et vältida autentimata kasutajate ligipääsu, andmekadu ja keskkonna väärkasutamist. Moodle veebilehel on turvalisuse ja privaatsuse tagamiseks välja toodud hulk erinevaid süsteemiüleseid üldiseid soovitusi, mis kuuluvad süsteemiadministraatori tegevusvaldkonda, kuid on süsteemi turvalisuse jaoks väga olulised:

- tee regulaarselt varukoopiaid;
- tee regulaarseid süsteemiuuendusi;
- kasuta Moodlet ainult kaitstud https protokolliga;
- kasuta tugevaid paroole;
- loo õpetaja kontosid ainult usaldusväärsetele kasutajatele;
- hoia süsteemid üksteisest lahus. Kasuta erinevaid keskkondi, erinevaid servereid.

17 https://docs.moodle.org/32/en/About_Moodle
18 https://docs.moodle.org/32/en/Security

Kuna Moodle on suletud e-õppe keskkond, peab selle kasutamiseks olema loodud kasutajakonto. HITSA[19] poolt pakutavasse Moodlesse on arendatud lisaks kasutajanime ja parooliga autentimisele ka turvaline Mobiil-ID ja ID-kaardiga autentimine.

Käesoleva töö raames uuritakse Moodle[20] õpikeskkonna kasutuspõhimõtete ploki all olevaid seadistusi. Moodle kasutuspõhimõtete sätted paneb paika peaadministraator. Nende koolide jaoks, kes kasutavad HITSA Moodlet, on see inimene HITSAs töötav inimene ja koolis neid sätteid keegi muuta ei saa. Oma kursuse piires saab kursusel osalejaid lisada ja eemaldada õpetaja. Vt Moodle (HITSA Moodle näitel) turvalisuse- ja privaatsuse sätteid lisast 1, punktist 1.

5.2 eKool

eKooli nimetati teistest õppeinfosüsteemidest kõige rohkem - 99 korda. eKool[21] on veebipõhine õppeinfosüsteem, mis ühendab endas kodu, kooli ja omavalitsust. eKool aitab õpilasel paremini õppida, lapsevanemad saavad olla paremini kursis sellega, kuidas nende lastel läheb ja kohalik omavalitsus omab head ülevaadet tema haldusalas olevate koolide toimimise kohta. eKool on Eesti esimene ja suurim veebipõhine õppeinfokeskkond - rohkem kui 200 000 aktiivset kasutajat ja miljon hinnet päevas. eKooli veebiversioon on õpilastele, vanematele ja õpetajatele tasuta. Tasuta teenust on võimalik pakkuda tänu eKooli keskkonnas kuvatavatele valitud reklaamidele.

eKooli[22] oluliseks osaks on klassipäevik, milles on õpetaja poolt sisestatud hinded, tunni sisu kirjeldused, kodused ülesanded, puudumised, hilinemised, märkused ning kontrolltööde ajad. Õpetaja sisestatud andmed (hinded, puudumised, kodutööd jm) muutuvad koheselt kõigile asjaosalistele kättesaadavaks. eKool on mobiili ja veebi kaudu kättesaadav kus iganes ja millal iganes, muutused on nähtavad reaalajas. Kõik kooli õpilased on automaatselt eKooli kasutajad, ligipääsud loob neile kooli IT-osakond kellele omakorda on vastavad õigused andnud eKooli arendajad. Lapsevanematel tuleb eKooli kasutamiseks täita (iga lapse kohta eraldi) liitumisankeet, misjärel loob ka lapsevanemale konto kooli IT-töötaja. Süsteemi logimiseks on 3 võimalust: ID-kaardiga; internetipanga kaudu; parooliga. Parooli saab luua omale nii õpilane kui lapsevanem ise, sisenedes ID-kaardi või internetipanga kaudu ja avades menüü sätted.

19 https://moodle.hitsa.ee/
20 https://docs.moodle.org/32/en/Security
21 https://www.ekool.ee/index_et.html
22 http://www.viimsi.edu.ee/failid/ekool_voldik.pdf

eKooli[23] kliendiandmete töötlemise põhimõtetes, on kirjas, et eKool ei saa tagada kliendiandmete turvalisust ega ole selle eest vastutav juhul, kui kliendiandmed ei ole kaitstud kliendi kasutatavate seadmete ebaturvalisuse tõttu või kui kolmandale isikule on saanud eKoolist sõltumatult teatavaks kliendi teenusega seotud kasutajaandmed või muu enda identifitseerimiseks kasutatav info või infokandja seega peab iga eKooli kasutaja tagama, et tema kasutajatunnused ei saaks kõrvalistele isikutele teatavaks.

eKooli[24] privaatsust käsitlevas dokumendis on öeldud, et juhul, kui sisestad oma profiili valeandmeid, nt võõra e-posti aadressi, võid oma konto teha nähtavaks isikule, kelle andmed need on. Arusaamatuste vältimiseks palutakse tähelepanelikult kontrollida oma isikuandmete õigsust. eKooli parool peab olema vähemalt 8 märki pikk ning sisaldama tähti ja numbreid. Unustatud parooli uuenduse saab tellida „Unustasid parooli?“ lingilt, millele klõpsates saadetakse kontoga seotud e-posti aadressile link uue parooli määramiseks. Link on kasutatav 3 tunni jooksul.

eKooli turvalisuse ja privaatsuse sätteid saavad kasutajad muuta vaid väheses mahus. Täpsemaid võimalusi vaata lisast 1, punktist 2.

5.3 Facebook

Facebook oli kõige enam nimetatud keskkond selliste seas, mida ei saa käsitleda klassikalise e-õppe keskkonnana, kuid seda vastavalt kohandades, saab selles õppetegevusi läbi viia. Facebooki nimetati uuringus 116 korral. Küsimuses, millega selgitati keskkondades esinevaid probleeme, nimetati kõige enam Facebooki. Välja toodi konto kaaperdamist, soovimatuid reklaame, tundmatute isikute sõbrakutseid, spämmi kirju ja muud taolist.

Facebooki[25] saab õppetöös kasutada näiteks kas suletud või avatud grupi (kursuse loomiseks) ja jagada seal õppematerjale, viia läbi arutelusid, küsitlusi ja teste. Facebooki kasutamiseks õppetöös on Inglismaa Hariduse Sihtasutuse poolt välja antud 20 leheküljeline materjal *Facebook guide for Educators* (Inglismaa Hariduse Sihtasutus, aastaarv puudub).

Facebookis liigub viiruseid, millest tasub teadlik olla. Veebilehel viirused.ee[26] kirjeldatakse üheksat Facebooki kaudu levivat viirust. Viiruste vältimiseks on samal veebilehel jagatud peamiseks nõuandeks seda, et tundmatutele linkidele ei tohi klikkida. Samuti, kui saate kelleltki sõnumi kahtlase lingiga, siis enne sellele vajutamist küsige saatjalt üle mis see on.

23 https://www.ekool.eu/terms/data_processing_principles_et.html
24 https://www.ekool.eu/terms/privacy_et.html
25 https://www.facebook.com/
26 http://viirused.ee/facebook-viirus/

Lisaks tuleks vältida iga mängu või muu rakenduse kasutamist Facebooki kaudu, sest ka seda võidakse häkkida. Kui Te olete langenud ükskõik millise Facebooki viiruse ohvriks, siis peaksite kohe muutma oma Facebooki salasõna, et vältida identiteedivargust.

Andmekaitse Inspektsiooni kodulehel[27] on pakutud nõuandeid kümne erineva turvalisuse ja privaatsuse probleemi lahendamiseks. Näiteks peaks ebasobivast sisust (ka ebasobivatest fotodest) teada andma Facebooki halduritele. Samuti tuleks Facebooki halduritele teada anda kui on kahtlus, et on loodud sinu nimeline libakonto ja kui tõe-poolest on tegemist identiteedi vargusega, tuleks sellest teavitada ka politseid. Palju saad aga ära teha ka ise, üle tasub vaadata oma isiklikud andmed, sätted, mis puudutavad seda kes ja kui palju minu infot näevad ning ka piirata otsingutulemustesse oma info kuvamist.

Facebooki saab logida parooliga, lisaks on võimalik kasutada erinevaid võimalusi kahekordseks autentimiseks, mille kohta saab täpsemalt lugeda lisas 1, punktis 3.

5.4 Kahoot

Kahooti nimetati kõige enam õpet toetavate keskkondade seas – kokku 178 korda. Kahoot[28] võimaldab õpetajatel ja õpilastel teha koostööd ning luua ja jagada teadmust nii klassiruumis kui selle väliselt. Kahoot on veebipõhine mängulist õpet pakkuv keskkond, mis töötab hästi ka nutivahenditel. See ei ole otseselt sotsiaalmeedia vahend, kuid seda kasutatakse lisaks haridusele ka sünnipäevadel, pulmades ja muudel suurüritustel. Kahootis saab luua nelja tüüpi mänge – test, hääletus, arutelu ja „järjesta“ tüüpi küsimusi. Nende loomiseks peab olema loodud ka kasutajakonto (sisse saab logida parooliga), kuid mängu mängimiseks piisab vaid sisenemisest keskkonda ja sisestada sinna mängu loonud inimese poolt antud mängu kood. Keskkonda konto loomisel küsitakse sünniaega, kasutajanime, meiliaadressi ja parooli. Kahooti mängimisel ei kogu Kahoot mingeid isikuandmeid. Küll aga konto loomisel saadetakse tutvumiseks Kahooti turvalisuse ja privaatsuse tingimused, mille järgi annate keskkonda oma isikuandmete sisestamisega automaatselt loa neid töödelda vastavalt turvalisuse ja privaatsuse tingimustes toodud sätetele. Alla 13 aastastelt lastelt ei koguta mingit muud infot, kui ainult sünniaega, kasutajanime, parooli ja e-maili aadressi. Viimast ainult selleks, et saata parooli uuendus, kui see on ununenud. Teistelt rollidelt võib Kahoot koguda ka muud infot. Saadud andmeid võib Kahoot kasutada näiteks uudiskirjade või reklaamise saatmiseks; teenuse muutmise kohta info edastamiseks; teenuse parandamiseks, analüüsiks, pettuste tuvastamiseks ning ennetamiseks ja audititeks. Andmeid võidakse avaldada kolmandatele osapooltele näiteks neile, kes pakuvad Kahootile majutuse ja hoolduse teenust,

27 http://www.aki.ee/et/uudised/uudiste-arhiiv/kuidas-kaitsta-oma-andmeid-facebookis
28 https://getkahoot.com/support/faq/

analüüsi, klienditeenindust, e-posti haldust, auditeerimist jms. Täiskasvanu saab esitada avalduse oma lapse ja enda kohta kogutud andmete vaatamiseks, parandamiseks, ajakohastamiseks, varjamiseks või kustutamiseks. Kasutaja saab loobuda turundusliku sisuga e-mailide saamisest, vajutades e-kirjas olevale listist eemaldamise taotluse lingile. Kahooti mängu loomisel saab valida kas see on avalik – kättesaadav kõikidele Kahooti kasutajatele või on see privaatne. Valik sisestatakse mängu loomisel. Alla 16 aastased lapsed ei saa luua ega otsida avalikke mänge. Samuti ei saa nad ise jagada mänge ega kasutada jagatud mänge küll aga saavad mängida neid mänge, mille koode nad teavad ja saavad ka oma mängu koodi teistele öelda. Ühe erisusena alla 16 aastaste laste kontode puhul on veel see, et nad ei saa sisse logimisel kasutada e-posti aadressi vaid peavad sisse logima kasutajanimega. Täpsemaid sätteid vaata lisast 1, punktist 4.

5.5 Google drive

Google drive võimaldab andmeid hoida Google serverites. Google drive rakendust kasutades tekib kaust nii kasutaja arvuti kõvakettale kui Google serverisse ja kaustas olevatele failidele pääseb ligi iga seadmega, mis võimaldab internetiühendust. Kaustas olev fail on alati sünkroniseeritud kõikide kontoga ühenduses olevate seadmetega (Aasamäe, 2012).

Google drive keskkonda nimetati küsitluses 358 korral. Google drives[29] on mugav teha ühistööd. Kas töötada välja koos mõnd dokumenti või lisada sinna dokument kellelegi ülevaatamiseks ja kommenteerimiseks. Algselt on loodud dokumendid privaatsed ja nähtavad ainult selle loojale. Dokumente saab aga teiste kasutajatega jagada. Jagamiseks on kolm võimalust – dokumendi saab määrata avalikuks, nii, et igaüks, kui ta selle otsinguga veebist leiab, saab sellele ligi või saab võtta jagamiseks dokumendi lingi – siis pääseb dokumendile ligi igaüks, kellel on link ja kolmandaks saab dokumendile ligipääsu anda vaid konkreetsele inimesele läbi tema meiliaadressi. Lisaks saab määrata kas edastatav dokument on saajale ainult vaatamiseks, kommenteerimiseks või saab ta seda ka muuta. Google drive keskkonda saab üles laadida ka näiteks MS Wordis tehtud dokumente.

Kuna Google drive on osa Google üldisest kontost, siis kehtivad sellele samad turvalisuse ja privaatsuse tingimused, mis üldiselt tervele Google kontole. Täpsemaid

[29] https://www.google.com/drive/

sätteid ja nende kasutussoovitusi vaata lisast 1, punktist 5.

Alljärgnevalt on kõikide kirjeldatud keskkondade kohta koostatud üldine ülevaatetabel (Tabel 5), lähtudes Euroopa Liidu andmekaitse direktiivis (1995) toodud peamistest privaatsuse riivet puudutavatest probleemidest. Lisaks on välja toodud ka keskkondadesse autentimise võimalused.

Tabel 5 Keskkondade kasutustingimused

	Moodle	**eKool**	**Face-book**	**Kahoot**	**Google drive**
Autentimine	Parool ID kaart m-ID	Parool ID kaart m-ID Panga-link	Parool 2x autenti-mine	Parool	Parool 2x autenti-mine
Alaealistele kasutajatele kitsendatud privaatsuse sätted	-	-	x	x	x
Kasutajale selgitatakse milliseid andmeid tema kohta kogutakse	-	x	x	x	x
Kasutajale selgitatakse mis otstarbel tema andmeid kogutakse	x	x	x	x	x
Kasutajale selgitatakse mis tingimustel tema andmeid edastatakse kolmandatele osapooltele	x	x	x	x	x
Kasutajale selgitatakse kuidas tema andmeid kaitstakse	-	-	x	x	x
Kasutajal on võimalus küsida mis andmeid tema kohta kogutud on ja neid vajadusel muuta lasta	x	x	x	x	x
Kas on kirjas, kes vastutab andmete kasutamise eest	Kasutaja	Kool ja kasutaja	Kasutaja	Kasutaja	Kasutaja
Turvalisuse ja privaatsuse sätted	Vaata lisa 1 pt 1	Vaata lisa 1 pt 2	Vaata lisa 1 pt 3	Vaata lisa 1 pt 4	Vaata lisa 1 pt 5

Kokkuvõtteks on tegemist viie väga erineva keskkonnaga. Kui Moodle ja eKool on keskkonnad, mis on spetsiaalselt loodud õppimisega seotud keskkondadeks, siis on ka nende turvalisuse poliitika vastavalt üles ehitatud. Turvalisuse ja privaatsuse sätted on seatud võimalikult rangeks, et andmed kuidagi ei lekiks ja kasutajatele endale pole ka

antud võimalusi neid sätteid oluliselt muuta.

Facebook, Kahoot ja Google on aga äriettevõtted, mis teenivad oma kasutajaskonnaga tulu ja sellest tulenevalt on nende algsed vaiksesätted jäetud üsna vabadeks ja kasutaja peab ise hoolsalt kasutustingimusi jälgima ja sätteid vajadusel rangemaks muutma.

Kahoot on oma funktsionaalsuselt väga väike ja ei kogu mingeid erilisi andmeid kasutajate kohta. Alla 13 aastastelt ei kogu üldse isikuandmeid ja üle 13 aastastelt saadud andmeid kasutatakse peamiselt individualiseeritud reklaamide saatmiseks või keskkonna parendamiseks.

Facebookil on päris palju privaatsusega seotud sätteid, mida kasutaja saab muuta, et oma privaatsust tagada. Sätete muutmisega saab vältida ebasoovitavat sisu ja isegi viiruste levimist.

Sama on Googlega – kasutajal on võimalik mitmeid sätteid muuta, et kaitsta oma privaatsust. Google drive küll (erinevalt teistest Google rakendustest, nt Google maps, photos, youtube, gmail, play, chrome jm) ei edasta kasutajatele reklaame ega kasuta muud moodi inimeste turvalisust ja privaatsust ära. Drive rakenduses on Google kõrge prioriteet kaitsta inimeste sisestatud dokumente.

6 Arutelu ja järeldused

Teoreetiliste materjalide läbitöötamisel leidis autor, et õpetajate ja õpilaste digipädevuste kasvu panustatakse täna Eestis kasvava trendina, kuid seda peamiselt selles suunas, et õpetajad tooksid õppetöösse sisse digivahendeid, kasutaksid erinevaid e-keskkondi, kombineeriksid e-õpet klassikalise kontaktõppega ja toodaksid kvaliteetseid e-õppematerjale (vt pt 1). Vähem räägitakse turvalisuse pädevustest, kuigi need on pädevusmudelites sõnastatud ja ka riiklikesse õppekavadesse sisse kirjutatud. Näiteks eeldatakse õpilastelt seda, et nad arvestaksid digitegevustes teiste inimeste privaatsusega ja ühiste kasutustingimustega ning kaitseksid oma isikuandmeid ja ennast veebipettuste, ohtude ning küberkiusamise eest (vt pt 1.1). Õpetajatelt eeldatakse, et nad soovitaksid, edendaksid ja õpetaksid digitaalse teabe ja tehnoloogia turvalist, seaduslikku ja eetilist kasutamist (vt pt 1.2).

Digipädevuste nõuded ei ole tekkinud niisama, vaid kogu turvalisuse teema on aasta-aastalt maailmas muutunud ja on veelgi muutumas järjest olulisemaks. Järjest enam võetakse kasutusele erinevaid e-keskkondasid, kasutatakse erinevaid rakendusi, nutiseadmeid ja suheldakse sotsiaalmeedias ka e-õppe tundide ja tegevuste läbiviimisel (vt pt 2.2). Samuti kasutavad rakenduste loojad ära kasutajate lohakat suhtumist turvalisuse ja privaatsuse sätetesse ning näiteks müüvad oma äri huvides klientide andmeid edasi kolmandatele osapooltele. Üldiselt annab iga rakendus kasutajakonto loomisel kasutajale tutvumiseks kasutustingimuste lepingu, millest peaks selguma mil määral kasutaja isikuandmeid kasutatakse ja mis võimalusi keskkond sätete muutmiseks pakub (vt pt 2.1). Kui keskkonna kasutustingimused tunduvad kasutajale kahtlased ja ei ole võimalik aru saada milliseid isikuandmeid kogutakse ja mis eesmärkidel, oleks mõistlik sellisesse keskkonda kasutajakontot mitte luua ja leida mõni selgemate tingimustega keskkond.

Magistritöö empiirilisest osast selgus, et valimis olnud koolides peetakse tänast e-õppe mahtu üldiselt optimaalseks, kuid trend on pigem kasvav. Samas võib eeldada, et e-õppe maht on koolides kasvamas, eriti kui arvestada, et valimis olid digitaalselt aktiivsed koolid. Digitaalselt madalama aktiivsusega koolid muutuvad aja möödudes

samuti aktiivsemaks ja ka neil korduvad suure tõenäosusega sarnased probleemid, mis täna esinevad digitaalselt aktiivsetel koolidel (vt pt 4.1).

Digipöörde programmid ja e-õppe arenemine üldiselt on toonud õppetöösse kasutusele palju e-keskkondasid. Uurimuses toodi õpilaste, õpetajate ja haridustehnoloogide poolt kokku välja 160 erinevat keskkonda, mida nad õppetöös kasutavad. Nende seas on nii e-õppe keskkondasid, õppeinfosüsteeme, õppematerjalide kasutamise ja ühistöö tegemise keskkondi, erinevaid rakendusi ja mänge, sotsiaalmeediakeskkondi, blogikeskkondi jne (vt pt 2.2). Keskkondade valik on lai ja on hea näha, et neid võimalusi ka kasutatakse. Samas tuleks erinevate keskkondade kasutuselevõtul arvestada sellega, et õpilased peavad ka kõikidesse nendesse keskkondadesse tehtud kasutajanimed ja paroolid meeles pidama või need kuhugi üles kirjutama. Kas nad suudavad kõik paroolid meeles pidada, panevad need päevikusse kirja, või kasutavad igas keskkonnas sama parooli, ei olnud selle uurimuse fookus, kuid igal-juhul ei ole esimene neist valikutest kuigi reaalne ja kaks järgmist ei ole kuigi turvalised. Seega tuleks koolides kindlasti õpilastele anda nõuandeid paroolide loomise ja ka nende säilitamise osas. Soovitada võiks selliseid keskkondi, kuhu saab sisse logida kas ID-kaardi või m-IDga ja kasutada kahetasandilist autentimist, kus see võimalik on (vt pt 2.2).

Kuigi üldiselt loovad õpilased keskkondadesse kontosid ise, selgus uurimusest, et abi vajavad nad kõige enam just paroolide taastamise osas. Ja samas küsimuses jäävad nad ka kõige enam ilma abita sest õpetaja võimuses ei ole õpilase konto taastamine või uue parooli tellimine. Nii, et sageli tuleb samasse keskkonda luua uus konto. Palju vajatakse abi ka keskkondadesse konto loomisel ja keskkonna kasutamisel. Täpselt samuti, samades asjades, jäävad ka õpetajad õpilaste nõustamisel hätta. Õnneks leiavad õpetajad abi kas oma kooli haridustehnoloogilt, IT-töötajalt või teiselt kolleegilt. Vahel otsitakse abi ka Internetist (vt pt 4.3).

Uuringust torkas silma sage sotsiaalmeedia kasutus. Kõige rohkem turvalisusega ja privaatsusega ette tulnud probleeme esines just Facebooki kasutamisel (vt pt 4.2). Seega, isegi, kui Facebooki ei kasutata otseselt õppetöö läbiviimiseks, võiks koolis mõne arvutitunni või muu sobiva tunni sisuks olla Facebooki turvalisuse ja privaatsuse sätete läbiarutamine, järgides näiteks käesoleva magistritöö tulemusena valminud turvalisuse ja privaatsuse sätete kasutamise nõuandeid (Lisa 1). Facebookil on palju

selliseid sätteid, mida kasutaja saab ise reguleerida, seega selline sätete üle arutlemine aitaks õpilastele kas meenutada või meeles pidada, et sellised sätted, millega on võimalik oma turvalisust ja privaatsust kaitsta, on olemas enam-vähem igas e-keskkonnas ja eriti tuleb nendele tähelepanu pöörata avatud keskkondades.

Uuringust selgus, et õpilased eelistavad pigem suletud keskkondasid või siis ka vastavalt vajadusele kombineeritud keskkondasid (vt pt 4.1). Selline eelistus viitab suuremale privaatsuse vajadusele ja tasub mõelda sellele, kuidas avatud keskkondade kasutamine võib õpilaste õpikäitumist mõjutada. Autor võib tuua tuua näite isiklikust kogemusest, avalikus blogis teiste õpilaste tööde kommenteerimise kohta, mida autor tegi nii minimaalselt kui võimalik, kuid nii palju kui vajalik kursuse läbimiseks. Sama oli ka avalikus blogis oma kodutööde avaldamisega. Teades, et need tööd on kättesaadavad kogu maailmale, et nende üleslaadimise hetkest võib need keegi kohe omale alla laadid, sai ka neisse kirja vaid minimaalne ja üldine arvamus. Pärast kursuse lõppemist muutis autor keskkonnas, kuhu nõuti kodutööde lisamist, selle keskkonna privaatsussätteid ja piiras kodutöödele ligipääsetavust. Avatud keskkonnas õppetöö läbiviimise peab väga hästi läbi mõtlema, et mitte vähendada õpilaste motivatsiooni ja põhjustada negatiivset õpikogemust. Samuti tuleks arvestada, et õpilaste avalikult esitatud mõtteavaldused ja kodutööd võivad neile tekitada soovimatut digijälge, mis võib tulevikus vähendada nende võimalust kandideerida mõnele töökohale. Avalikult esitatud tööd võivad tekitada ka ohu, et neid hakatakse koolikaaslaste poolt kiusama, kuna töö oli kas liiga nõrk, ebasobival teemal või hoopis liiga hea.

Oma teadlikkust e-keskkondades valitsevatest ohtudest peavad pigem heaks nii õpilased kui õpetajad, samuti peetakse turvalisuse ja privaatsuse sätete muutmise võimalusi olulisteks, kuid ikkagi esineb näiteks Facebookiga (kus saaks väga palju oma turvalisuse ja privaatsuse kaitseks ära teha) probleeme ja õpilased tunnistavad ka seda, et tegelikult nad tutvuvad sätetega vaid mõni kord või siis pigem üldse mitte. Õpetajate ja haridustehnoloogide osas on olukord veidi parem, nad väidavad, et nad pigem tutvuvad keskkondade privaatsussätetega. Kuna üldjuhul luuakse uude e-keskkonda kasutajakonto kontakttunnis koos õpetajaga, siis võiksid õpetajad konto loomisel koos õpilastega üle vaadata keskkonna kasutamise leping ja uurida turvalisuse sätteid. Arvestades, et praegused, nii õpilaste kui õpetajate poolt väljatoodud põhjendused, miks nad sageli sätetega ei tutvu, on pigem seotud sellega,

et otseselt väga suuri probleeme pole veel eriti paljudel ette tulnud, seega lihtsalt ei pöörata nendele tähelepanu ja ei raisata nende lugemisele aega. Samuti selgus pime usaldus, et kui paljud teised kasutavad mingit keskkonda, siis õpetajad järeldavad, et see on turvaline, haridustehnoloogid aga eeldavad, et õpetajad ise tutvuvad keskkondade sätetega. Seega kui kumbki pole sätetega tutvunud, võibki juhtuda, et postitatud materjalid on kogu maailmale nähtavad (vt pt 4.2).

Üldisemalt avaldati toe osas soovi saada teadlikkumaks e-keskkondade turvalisuse ja privaatsuse probleemide osas, mis võivad tekitada õpilastele soovimatut digijälge. Mainiti ka vajadust saada lisainfot keskkondade turvalisuse ja privaatsuse sätete osas (vt pt 4.3).

Enamlevinud keskkondade turvasätete analüüsist selgus, et selliste teenusepakkujate poolt, kes pakuvad koolidele teenust lepingu alusel, vastutavad turvalisuse ja privaatsuse tagamise eest ise ja on seega ka võimalikud sätted turvaliselt ära seadistanud, jätmata kasutajatele – õpetajatele ja õpilastele, erilise võimaluse neid sätteid muuta. Sellisteks on näiteks Moodle ja eKool. Seevastu Facebooki sätetes on palju, mida kasutaja peaks teadma ja ise muutma, sest selle keskkonna eesmärk ei ole tagada kellegi privaatsust, vaid pigem soodustada info levikut ja sotsiaalset suhtlemist, jättes selle otsustuse, kui palju ta oma andmeid kaitseb, kasutaja poolele. Kui õpilased on enamjaolt harjunud Moodle ja eKooliga, kus probleeme ei esine nii palju kui nt Facebookis ja nad midagi ise seadistada ei saa, ei ole väga imeks pandav, et nad ei taipa neid sätteid vaadata ka teistes keskkondades, seetõttu ka enamus väljatoodud probleeme puudutavad just avatud keskkondi, kus andmete avalikustamise mahu otsustus on nende endi käes, mitte teenusepakkuja käes. Ka Google drive ja e-õppes kasutatavate väiksemate rakenduste sätteid tasub kasutajal üle vaadata, olemaks veendunud, et keskkonda konto loomisel ja tingimustega nõustumisel (mida sageli ei loeta), ei avaldataks enda kohta liiga palju infot, mis võib põhjustada turvalisuse või privaatsuse probleeme (vt pt 5).

Kokkuvõte

Õpetaja võttis kasutusele uue e-keskkonna. Kasutajakonto loodi õpetaja juhendamisel kontakttunnis. Samal ajal tutvuti ka keskkonna kasutustingimuste ning turvalisuse ja privaatsuse sätetega. Õpetaja juhtis tähelepanu, et kui nad postitavad keskkonda oma essee, saavad nad määrata, kellele see töö nähtav on – kas ainult õpetajale või kõikidele klassikaaslastele. Õpilastele oli nõuanne arusaadav ja kellelgi ei tekkinud probleemi sellega, et nende poolt esitatud töö oleks olnud kättesaadav nendele, kellele nad seda avaldada ei soovinud.

Selline oleks ideaalne stsenaarium, lähtuvalt käesoleva magistritöö tulemusena selgunud vajadustest. Selliste vajadusteni jõuti läbi tööle püstitatud eesmärgi ja uurimisküsimuste.

Töö eesmärgiks oli jõuda soovitusteni, millele koolides kasutusel olevate e-keskkondade turvalisuse- ja privaatsussätete juures tähelepanu pöörata.

Uurimisküsimusteks olid:

- Kas Eestis kehtivatesse digipädevuste nõuetesse on sisse kirjutatud turbe teemalisi pädevusi?
- Milliseid e-õppe keskkondasid Eesti koolides kasutatakse ja milliseid probleeme on nende kasutamisel ette tulnud?
- Millised on nende keskkondade turvalisuse- ja privaatsuse sätted ning kuidas neid sätteid kasutada, et oma turvalisust ja privaatsust kaitsta?

Eesmärgi saavutamiseks ja empiirilise uurimuse läbiviimiseks analüüsiti töö esimestes kahes peatükis õpilaste ja õpetajate turbeteemalisi digipädevusi, erinevat tüüpi e-keskkondade positiivseid ja negatiivseid külgi ning käsitleti turvalisuse ja privaatsuse temaatikat üldiselt. Analüüsist selgus, et õpilaste ja õpetajate digipädevusi küll tõstetakse, kuid üldiselt ei pöörata tähelepanu turvalisust tõstvatele pädevustele.

Töö kolmandas peatükis toodi välja uurimismeetodid ja kirjeldati valimit. Andmete kogumise meetodiks valiti küsitlusankeet, mis võimaldas saada võimalikult laialdase tagasiside.

Töö neljandas peatükis võeti kokku ankeetküsitluse käigus selgunud tulemused. Üldiselt toetasid tulemused ka teoreetilisi andmeid, kuigi arvestades turvalisuse ja privaatsuse temaatika olulisust teoorias, eeldas autor, et vastajad on turvalisuse probleemide ja privaatsuse riivamisega rohkem kokku puutunud, kui küsitluses välja toodi.

Viiendas peatükis analüüsiti ka ankeetküsitlusest selgunud enamkasutatavate e-keskkondade turvalisuse ja privaatsuse sätteid. Küsitluses nimetati kokku 160 erinevat keskkonda. Autor jagas üle kümne korra nimetatud keskkonnad funktsionaalsuse järgi viide gruppi: e-õppe keskkonnad, õppeinfosüsteemid, õppetööks kohandatavad keskkonnad, õppematerjalide jagamise keskkonnad ja e-õpet toetavad rakendused ning analüüsis igas grupis kõige rohkem nimetatud keskkondade kasutustingimusi ning turvalisuse ja privaatsuse sätteid. Iga sätte juurde lisas autor kas omapoolse või keskkonna loojate poolt antud soovituse sätte kasutamiseks.

Uurimusele püstitatud eesmärgi saab lugeda täidetuks – töö tulemusena on lisas 1 välja toodud enamkasutatavate e-keskkondade turvalisuse ja privaatsuse sätted koos nende kasutamise soovitustega.

Edasisteks uurimisvõimalusteks samas valdkonnas võiks olla sarnase uurimuse läbiviimine näiteks kolme aasta pärast kui õpilastel ja õpetajatel on olnud võimalik tõsta ka oma pädevusi turvalisuse ja privaatsuse osas ja võrrelda neid tulemusi käesoleva magistritöö tulemustega. Kuna selgus, et paljud vastanud sooviksid rohkem infot saada oma digijälje vähendamise osas, siis võiks veel uurida millised on õpilaste kontode loomise harjumused (ja nende loomisel ka paroolide loomise ja hoiustamise harjumused), kui palju kontosid ja millistes keskkondades on keskmiselt ühel õpilasel/õpetajal/haridustehnoloogil ja kas ja kuidas nad omavad infot millisesse keskkonda nad on üldse kunagi konto loonud ning kas ja kuidas nad saaksid selle kustutada kui nad seda enam ei kasuta.

Summary

The topic of the thesis is: „Security and Privacy in the E-environments for Stage III of Basic Education and Upper Secondary Education“.

The goal of the thesis is, based on the feedback in surveys, to compile recommendations what to focus on in the security and privacy settings of the digital learning environments used in the schools.

Based on needs revealed by results of this masters thesis, the above is the ideal scenario. Understanding of the needs were reached through the survey, that focused on following questions:

- whether requirements of digital qualifications include topics of information security;
- what digital learning environments are being used in Estonian schools and what kind of problems has occurred;
- what are the security and privacy settings for those environments and how to use these settings to avoid problems in that domain.

To reach the goal of the task and for conducting the empirical research, in the first two chapters analysis covers teachers and students security oriented awareness, positive and negative aspects of different digital learning environments and touches in broader sense on security and privacy topics. Analysis reveals that digital qualifications of teachers and students are being raised, but is less focused on security related topics. A theoretical part of the thesis reveals an observation, that use of open environments is gaining popularity.

Third chapter describes the methodologies used in the research and explains the properties of the survey sample. A questionnaire was chosen as the mean of the survey, which enabled wide selection of responses. Questionnaire was filled in 507 times.

Fourth chapter summarises the survey results. Survey results largely supported the theoretical base, although considering the importance of security and privacy topics the author expected higher awareness on that topic than the result indicated.

Fifth chapter analyses the privacy and security settings of the most commonly used digital learning environments. In total of 160 different environments were mentioned in the survey results. Author selected environments mentioned more than on 10 occurrences and bucketed them based on the functionality into 5 categories : digital learning environments, learning management systems, digital environments that can be adapted for learning, learning materials distributions systems and applications that support digital learning. Each bucket was analysed for usage agreement criteria and security and privacy settings. For each setting author added usage recommendations based on her own experience or used environment creators recommendations.

Goal of the study can be declared successfully achieved - privacy and security settings enlisting, together with usage recommendation for most used digital learning environments is resulted in appending #1 in the thesis. Wider goal of raising awareness of the topic, can be achieved by distributing the publication of this work.

Suggestions for further research in this domain are repeating similar research in 3 years - the time students and teachers have had time to increase their qualifications on privacy and security - and compare the results with this thesis. The study revealed, that many would like to learn more about reducing their digital footprint. That suggests that additional study about practices of new account creation and credentials management would be beneficial. Also it would be useful to research the number of accounts in which environments individuals have, do they have full awareness of existing accounts they have ever created and whether the accounts could be closed in case not being used.

Kasutatud allikad

Aasamäe, K. (2012). *Kogu tõde Google Drive'ist*. Loetud aadressil http://majandus24.postimees.ee/820202/kogu-tode-google-drive-ist

Adams, A., & Blandford, A. (2003). *Security and online learning: to protect or prohibit*. Loetud aadressil http://oro.open.ac.uk/11919/1/18_Chap_Adams_%281%29.pdf

Adetoba, B.T., Awodele, O.,& Kuyoro, S.O. (2016). *E-learning security issues and challenges*. Loetud aadressil http://www.modernrespub.org/jsrs/pdf/2016/May/Adetoba%20et%20al.pdf

Andmekaitse Inspektsioon. (2016). *Kuidas kaitsta oma andmeid Facebookis?* Loetud aadressil http://www.aki.ee/et/uudised/uudiste-arhiiv/kuidas-kaitsta-oma-andmeid-facebookis

Andrejevic, M. (2009). *Privacy, Exploitation, and the Digital Enclosure.* Loetud aadressil http://amsterdamlawforum.org/article/view/94/168

Bandara, I., Ioras, F. & Maher, K. (2014). *Cyber security concerns in e-learning education*. Loetud aadressil http://ecesm.net/sites/default/files/ICERI_2014.pdf

Broadbent, B. (2002). *ABCs of e-learning. Reaping the benefits and avoiding the pitfalls*. Loetud aadressil http://elearn.uzulu.ac.za/index.php/types-of-e-learning

Cybernetica AS. (2011-2017). Andmekaitse ja infoturbe leksikon. Loetud aadressil http://akit.cyber.ee/

Cranon, L. (2016). *Time to rethink mandatory password changes*. Loetud aadressil https://www.ftc.gov/news-events/blogs/techftc/2016/03/time-rethink-mandatory-password-changes

Eesti Hariduse ja Teaduse Andmesidevõrk (EENet). (kuupäev puudub). *Akadeemilise andmeside areng Eestis*. Loetud aadressil https://www.eenet.ee/EENet/akadeemilise_andmeside_areng_Eestis

eKool. (kuupäev puudub). Loetud aadressil https://ee.ekool.eu/index_et.html

eKool. (kuupäev puudub). *Mis on eKool?* Loetud aadressil http://www.viimsi.edu.ee/failid/ekool_voldik.pdf

eKool. (kuupäev puudub). *Kliendiandmete töötlemise põhimõtted*. Loetud aadressil https://www.ekool.eu/terms/data_processing_principles_et.html

eKool. (kuupäev puudub). *Privaatsus*. https://www.ekool.eu/terms/privacy_et.html

Euroopa parlamendi ja nõukogu direktiiv 95/46/EÜ. (1995). EÜT L 281, 23.11.1995. Loetud aadressil http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CONSLEG:1995L0046:20031120:ET:PDF

Euroopa parlamendi ja nõukogu määrus 2016/679. (2016). Loetud aadressil http://eur-lex.europa.eu/legal-content/ET/TXT/PDF/?uri=OJ:L:2016:119:FULL&from=ET

European Commission. (2017). *Proposal for a European Framework for the Digital Competence of Educators.* Draft for Discussion.

European Commission. (2011). *Eurobaromeetri eriuuring 359*. Loetud aadressil http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_en.pdf

European Parliament. (2006). *Recommendation of the European Parliament and of the Council of 18 December 2006 on key competences for lifelong learning*. Loetud aadressil http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32006H0962

European Schoolnet. (kuupäev puudub). *Saa omale e-turvalisuse märgis*. Loetud aadressil http://www.esafetylabel.eu/web/guest/esafetyschool

Facebook. (kuupäev puudub). Loetud aadressil https://www.facebook.com/

Ghauri, P., & Gronhaug, K. (2004). *Äriuuringute meetodid. Praktilisi näpunäiteid*. Kirjastus Külim.

Google. (kuupäev puudub). Loetud aadressil https://www.google.com/drive/

Google Classroom. (kuupäev puudub). Loetud aadressil https://classroom.google.com/u/0/h

Gümnaasiumi riiklik õppekava. (2014). RT I, 29.08.2014, 21

Haridus- ja Teadusministeerium (HTM). (2014). *Eesti elukestva õppe strateegia 2014-2020*. Loetud aadressil https://www.hm.ee/et/elukestva-oppe-strateegia-2020

Haridus- ja Teadusministeerium (HTM). (2015). *Eesti elukestva õppe strateegia 2020*

digpöörde programm. Loetud aadressil https://www.htm.ee/sites/default/files/ministri_kaskkiri_digipoorde_programm_2015-2018.pdf

Hariduse Infotehnoloogia Sihtasutus (HITSA). (2016). *Õppijate digipädevuste mudel*. Loetud aadressil https://www.hm.ee/sites/default/files/digipadevuse_mudel_2016veebiuus.pdf

Hariduse Infotehnoloogia Sihtasutus (HITSA). (kuupäev puudub). *Digitaalselt aktiivne kool: kuldtase*. Loetud aadressil http://www.hitsa.ee/ikt-hariduses/digitaalselt-aktiivne-kool/kuldtase

Hariduse Infotehnoloogia Sihtasutus (HITSA). (kuupäev puudub). HITSA Innovatsioonikeskus. Loetud aadressil https://www.innovatsioonikeskus.ee/et/meist

Haridustehnoloogia sõnastik. (kuupäev puudub). *Wikipedia*. Loetud 06. jaanuar 2017 aadressil http://wiki.e-uni.ee/htsonastik/

Hisjärvi, S., Remes, P., & Sajavaara, P. (2010). *Uuri ja kirjuta*. Kirjastus Medicina

Inglismaa Hariduse Sihtasutus. (aastaarv puudub). *Facebook guide for Educators*. Loetud aadressil http://www.ednfoundation.org/wp-content/uploads/Facebookguideforeducators.pdf.

International Society for Technology in Education (ISTE). (2008). *Digipädevuste standard õpetajatele*. Loetud aadressil http://www.innovatsioonikeskus.ee/sites/default/files/ISTE/ISTE_NETS_T_2014.pdf

Kahoot. (kuupäev puudub). Loetud aadressil https://getkahoot.com/support/faq/

Kahoot. (kuupäev puudub). Loetud aadressil https://create.kahoot.it/login

Kampylis, P., Punie, Y., & Devine, J. (2015). *Promoting Effective Digital-Age Learning. A European Framework for Digitally-Competent Educational Organisations*. Loetud aadressil http://publications.jrc.ec.europa.eu/repository/bitstream/JRC98209/jrc98209_r_digcomporg_final.pdf

Kuhn, C. (2017). *Open or closed learning environments? The topography of HE*

practitioners learning spaces. Towards a topology of learning spaces. Loetud aadressil http://conference.oeconsortium.org/2017/presentation/open-or-closed-learning-environments-the-topography-of-he-practitioners-learning-spaces-towards-a-topology-of-learning-spaces/

Kusnets, K. (2007). *E-kursuste õppedisaini modelleerimine ja toestamine multimeediumipõhise õppematerjali abil eesti e-kutsekooli kontekstis* (magistritöö). Loetud aadressil http://www.cs.tlu.ee/teemaderegister

Laanpere, M. (2016). *DigiPeeegel: kooli digiküpsuse hindamisvahend*. Loetud aadressil https://www.innovatsioonikeskus.ee/sites/default/files/mart_laanpere.pdf

Laanpere, M. (aastaarv puudub). *Veebipõhise õppekeskkonna loomine ja kasutamine informaatika ainetundides*. Loetud aadressil http://oppekava.innove.ee/wp-content/uploads/sites/6/2017/01/Veebip%C3%B5hise_%C3%B5ppekeskkonna_loomine_ja_kasutamine_informaatika_ainetundides.pdf

Laanpere, M., Pata, K., Luik, P. & Lepp, L. (2016). *Õpetajate digipädevuste hindamismudeli uuringu aruanne*. Loetud aadressil http://www.innovatsioonikeskus.ee/sites/default/files/ISTE_hindamismudeli_uuringu_aruanne.pdf

Lorenz, B. (2017). *A Digital Safety Model for Understanding Teenager Internet User´s Concerns* (doktoritöö). Loetud aadressil http://www.etera.ee/zoom/30536/view?page=3&p=separate&view=0,0,2067,1841

Lorenz, B., Kikkas, K. (2014). *If I Do Not Like Your Online Profile I Will Not Hire You!* Loetud aadressil https://link.springer.com/chapter/10.1007/978-3-319-07485-6_42

Lorenz, B., Sousa, S., & Tomberg, V. (2013). *Privacy Awareness of Students and Its Impact on Online Learning Participation – A Case Study*. Loetud aadressil https://link.springer.com/chapter/10.1007/978-3-642-37285-8_21

Majandus- ja Kommunikatsiooniministeerium (MKM). (2014a). *Küberjulgeoleku strateegia 2014 - 2017*. Loetud aadressil https://www.mkm.ee/sites/default/files/kuberjulgeoleku_strateegia_2014-2017.pdf

Majandus- ja Kommunikatsiooniministeerium (MKM). (2014b). *Eesti infoühiskonna arengukava 2020*. Loetud aadressil https://www.mkm.ee/sites/default/files/elfinder/article_files/eesti_infouhiskonna_arengukava.pdf

Majandus- ja Kommunikatsiooniministeerium (MKM). (2016). *Toetuse andmise*

tingimused üldhariduskoolide digitaristu kaasajastamiseks. Loetud aadressil https://www.struktuurifondid.ee/sites/default/files/oigusaktid/toetuse_andmise_tingimused_uldhariduskoolide_digitaristu_kaasajastamiseks_06.04.2016.pdf

Mets, U., Nevsky, E., Pedaste, M., & Laanpere, M. *Digipädevus õppekavades* (2016). Loetud aadressil http://oppekava.innove.ee/digipadevus-oppekavades/

Miksike. (kuupäev puudub). Loetud aadressil http://www.miksike.ee

Moodle. (kuupäev puudub). Loetud aadressil https://moodle.hitsa.ee/

Moodle. (kuupäev puudub). *Moodlest.* Loetud aadressil https://docs.moodle.org/32/en/About_Moodle

Moodle. (kuupäev puudub). *Turvalisus*. Loetud aadressil https://docs.moodle.org/32/en/Security

Moodle. (kuupäev puudub). *HITSA Moodle*. Loetud aadressil https://moodle.hitsa.ee/

Murumaa-Mengel, M., Pruulmann-Vengerfeld, P., & Laas-Mikko, K. (2014). Loetud aadressil *http://www.humanrightsestonia.ee/wp/wp-content/uploads/2014/11/EST-Uuringu-IV-osa-tulemused1.pdf*

Oolo, E., & Siibak, A. (2013). *Performing for one's imagined audience: Social steganography and other privacy strategies of Estonian teens on networked publics*. Loetud aadressil http://www.cyberpsychology.eu/view.php?cisloclanku=2013011501&article=7

Põhikooli riiklik õppekava. (2014). RT I, 29.08.2014, 20

Riigi Infosüsteemi Amet (RIA). (kuupäev puudub, a). *Turvaintsidentidest teavitamise juhend*. Loetud aadressil https://www.ria.ee/public/CERT/Turvaintsidendist_teavitamise_juhend.pdf

Riigi Infosüsteemi Amet (RIA). (kuupäev puudub, b). *Riigi Infosüsteemi võtmepõhimõtted*. Loetud aadressil https://www.ria.ee/teejuht/elu-infouhiskonnas/riigi-infosusteemi-votmepohimotted

SA Innove. (2017). *Algasid ulatuslikud haridusega rahulolu küsitlused.* Loetud aadressil https://www.innove.ee/et/uudised/728/algasid-ulatuslikud-haridusega-

rahulolu-kusitlused

Siemens, G. (2004). *Learning Management Systems: The wrong place to start learning*. Loetud aadressil http://www.elearnspace.org/Articles/lms.htm

Steeves, V. (2009). *Reclaiming the Social Value of Privacy*. Loetud aadressil: http://www.idtrail.org/files/ID%20Trail%20Book/9780195372472_kerr_11.pdf

Targalt Internetis. (kuupäev puudub). Loetud aadressil http://www.targaltinternetis.ee/projektist/

Viirused.ee. (2017). *Facebook viirus. Kuidas seda eemaldada?* Loetud aadressil http://viirused.ee/facebook-viirus/

Võrguvara.ee. (kuupäev puudub). *Turvaline autentimine*. Loetud aadressil https://www.vorguvara.ee/turvaline-autentimine-1

Wordpress. (kuupäev puudub). Loetud aadressil https://wordpress.com

Wright, C., Lopes, V., Montgomerie, T., Reju, S., & Schmoller, S. (2014). *Selecting a Learning Management System: Advice from an Academic Perspective.* Loetud aadressil http://er.educause.edu/articles/2014/4/selecting-a-learning-management-system-advice-from-an-academic-perspective

ÕIS. (kuupäev puudub). Loetud aadressil http://ois.tlu.ee/pls/portal/ois2.ois_public.main

10 Monkeys. (kuupäev puudub). Loetud aadressil https://www.10monkeys.com/ee/

LISAD

Lisa 1 E-keskkondade turvalisuse- ja privaatsuse sätted ja soovitused nende kasutamiseks

1.1 HITSA MOODLE

ADMINISTRAATORI SÄTTED

Säte	Vaikesäte	Kirjeldus ja soovitus
Kaitse kasutajanimesid	Vaikimisi: Jah	Kui kasutaja on unustanud parooli ja tellib parooli uuenduse, siis ei kuvata talle seda, millisele meiliaadressile see uuendus saadetaks. Säte kaitseb selle eest, et kui keegi pahatahtlikult tellib sinu konto alt parooli uuenduse, siis ta ei saa teada millisele meiliaadressile see läks.
Sunni kasutajaid sisse logima	Vaikimisi: Ei	Kuna Moodlesse saab teha ka avalikke kursuseid, millel saab osaleda ilma sisselogimiseta, ei pea kõiki kasutajaid sundima keskkonda sisse logima. Kui aga Moodlet kasutatakse ainult suletud kursuste jaoks, võib sund-logimise sisse lülitada.
Profiili vaatamiseks peab olema sisse logitud	Vaikimisi: Jah	Selle sättega saab inimesi sundida sisenema reaalse kontoga (mitte külalisena). Kui seda sätet mitte kasutada, võib juhtuda, et mõni kasutaja postitab oma profiilile reklaame või muud sobimatut sisu, mis kuvatakse välja ka otsingumootorites. Kui kasutaja ei ole sisse loginud reaalse kontoga, ei ole tal võimalik ka teiste profiile vaadata.
Kasutajapiltide nägemiseks sunni kasutajaid sisse logima	Vaikimisi: Ei	Kui seda sätet mitte kasutada, siis peab arvestama, et reaalse kontoga mitte sisseloginud kasutajad ei näe ka teiste kasutajate profiilipilte.
Ava Google´s	Vaikimisi: Ei	Kui see säte on lubatud, võimaldatakse Moodlele külalisena ligipääsu Google konto kaudu. Arvestama peab, et see säte võimaldab

		nähtamatu juurdepääsu kursustele, kus külaliste juurdepääs on lubatud.
Profiili nähtavad rollid	Vaikimisi rollid, mis kuvatakse kasutajaprofiilis ja osalejate lehel, on: Õpetaja (toimetaja), Tuutor, Õppija, Vaatleja	Rollid mida saab juurde lisada, on: Manager (konkreetse kooli peakasutaja/haldur), Kursuse looja, Külaline, Autoriseeritud kasutaja, kes ei ole kursusele registreerunud, Administraator (HITSA töötaja). See säte tagab, et pahatahtlikud kasutajad ei tuvastaks milline teistest kasutajatest on näiteks Administraator. Kui lisaks rollile on nähtav ka tema kontoga seotud e-posti aadress, võib ta püüda Administraatori e-maili paroole ära arvata, et pääseda ligi Administraatori kontole.
Üleslaaditava faili maksimum-suurus	Vaikimisi: 1Gb	Selle sättega määratakse üleslaaditavate failide maht kogu Moodles. See säte tagab, et keskkonda ei laetaks üles liiga suuremahulisi faile mis võivad keskkonna tööd takistada.
Kasutaja ruumilimiit	Vaikimisi: 100Mb	Maht, mida kasutaja saab oma privaatses failialas talletada. Tagab selle, et kasutajad ei kasutaks Moodlet isiklike suurte failide hoiustamise kohana.
Luba sildid EMBED ja OBJECT	Vaikimisi on kasutusel turbemeede, et tavakasutajad ei saa manustada multimeediumi (nt Flashi objekte) teksti, kasutades oma HTML-koodis silte EMBED ja OBJECT (selle toimingu saab teha meediumilisandmoodulite filtri abil).	Selle säte keelamine tavakasutajatele tagab selle, et keegi ei saaks lisatud HTMLina lisada Moodlesse mõnd viirust sisaldavat sisu.
Luba usaldusväärne sisu	Vaikimisi puhastab Moodle alati teksti, mida kasutajad sisestavad, ja eemaldab kõik kahtlased/ohtlikud skriptid, meediumid jms, mis võivad põhjustada turberiske.	Võimalik on teatud usaldusväärsetele kasutajatele anda võimalus lisada neid funktsioone oma sisusse ilma vahelesegamiseta. Selle süsteemi lubamiseks tuleb esmalt lubada see säte ja seejärel anda kindlale Moodle rollile õigus Usaldusväärne sisu. Selles rollis olevate kasutajate loodavaid või üleslaetavaid tekste ei puhastata.

Õpikeskkonna kasutuspõhimõtte URL	Vaikimisi: pole määratud	Kui teie õpikeskkonnas on kindlaks määratud põhimõtted, millega kõik registreeritud kasutajad peavad enne tutvuma ja nõustuma, siis sisestage siin vastav veebiaadress, muudel juhtudel jätke see väli tühjaks. See väli võib sisaldada mis tahes avalikku veebiaadressi. Tegemist on kasutajate teavitamisega võimalikest turvalisuse ja privaatsuse sätetest.
Külalistele mõeldud õpikeskkonna põhimõtete URL	Vaikimisi: pole määratud	Kui teie õpikeskkonnas on kindlaks määratud põhimõtted, millega kõik külaliskasutajad peavad enne tutvuma ja nõustuma, siis sisestage siin vastav veebiaadress, muudel juhtudel jätke see väli tühjaks. See väli võib sisaldada mis tahes avalikku veebiaadressi. Tegemist on kasutajate teavitamisega võimalikest turvalisuse ja privaatsuse sätetest. Sisselogimata kasutajate juurdepääsu saab keelata sund-sisselogimise sättega.
Ainult registreerunud kasutajate profiilid	Vaikimisi: Jah	Rämpspostitajate eest kaitsmiseks on nende kasutajate profiilikirjeldused peidetud, kes pole ühelegi kursusele registreerunud. Uued kasutajad peavad registreeruma vähemalt ühele kursusele, et nad saaksid oma profiilikirjeldust muuta.
Mitu korda lubatakse sisestada valet kasutajanime ja parooli	Vaikimisi: pole määratud	Selle sättega saab määrata nurjunud sisselogimiskatsete arvu, mille järel konto lukustatakse. Selle sätte rakendamine kaitseb kasutajakontot parooli lahtimurdmise eest.
Konto lukustamise jälgimise aken	Vaikimisi: 30 min	Selle sättega saab määrata aja, mille möödudes lubatakse uuesti sisestada nii mitu korda parooli, kui see oli eelmise sättega lubatud.
Konto lukustamise kestus	Vaikimisi: 30 min	Saab määrata mitme minuti pärast suletud konto uuesti avatakse parooli sisestamiseks.
Parooli-põhimõtted	Vaikimisi: Jah	Selle sätte lubamisel hakkab Moodle kasutajate paroole võrdlema kehtivate paroolipõhimõtetega.

		Kui seda sätet muuta, siis eiratakse parooli sisestamisel allpool kehtestatud nõudeid.
Parooli pikkus, paroolis kasutatavad numbrid, väiketähed, suurtähed, sümbolid	Vaikimisi: 8	Paroolid peavad olema vähemalt nii mitu tähemärki pikad. Parooli pikkus võiks olla seadistatud vähemalt 14 tähemärgi pikkuseks. Parool peaks sisaldama vähemalt ühte numbrit, ühte suurtähte ja ühte sümbolit. Selliselt seadistatud parool on paremini kaitstud lahtimurdmise eest.
Järjestikuseid identseid märke	Vaikimisi: 0	Parool ei peaks sisaldama järjestikuseid identseid märke. Selle keelamiseks sisestage väärtus 0. Selliselt seadistatud parool on paremini kaitstud lahtimurdmise eest.
Parooli vaheldumise limiit	Vaikimisi: 0	See näitab, mitu korda peab kasutaja oma parooli muutma enne, kui tal on lubatud parooli uuesti kasutada. Tagab kasutaja parooli parema kaitse.
Maksimaalne aeg, mille jooksul peab parooli lähtestamise taotluse valideerima	Vaikimisi: 30 min	Sellega sättega määratakse aeg, mille jooksul tuleb parooli lähtestamise taotlus enne aegumist valideerida. Säte tagab selle, et kui keegi üritas murda sisse Moodlesse ja tellis parooliuuenduse, siis ei ole tal liiga palju aega, et sisse murda ka meilikontole, et kätte saada parooli uuendamise link.
Logi parooli muutmise järel välja	Vaikimisi: Ei	Kui see säte on lubatud, lõpetatakse parooli muutmise järel kõik brauseriseansid, v.a seanss, kus uus parool määrati. Sellega tagatakse, et muudetud parooli järgselt ei oleks eelmise parooliga võimalik enam avatud sessioonide kaudu toiminguid teha.
Rühmapõhise registreerimise võtme tingimused	Vaikimisi: Jah	Selle sätte lubamisel hakkab Moodle rühma võtmete määramisel kontrollima vastavust kehtivatele paroolipõhimõtetele. Kui seda sätet mitte kasutada, ei kontrollita kas rühmale määratud paroolid vastavad paroolipõhimõtetele.
Meiliaadressi	Vaikimisi: Jah	Nõua meili teel kinnitamist, kui kasutaja

muutmise kinnitus		muudab oma profiilis meiliaadressi. Kui see säte on sisse lülitatud, saad oma kontot kaitsta selle eest, et kui keegi on pahatahtlikult su kontol meiliaadressi muutnud, siis ei saa ta seda kinnitada (kui ta ei pääse ligi su meilikontole).
Jäta kasutajanimi meelde	Vaikimisi: valikuline	Kasutajanime meelde jätmist ei ole soovitav sisse lülitada, vältimaks automaatset sisse logimist kellegi teise poolt, kui tal on ligipääs sinu seadmele (arvuti, telefon vm)

ÕPETAJA SÄTTED

Säte	Vaikesäte	Kirjeldus ja soovitus
Kas kursus on õppijatele nähtav?	Vaikimisi: Peida	Kui soovid kursust õppijatele nähtavaks teha, tuleb valida säte „Näita“.
Luba külalise ligipääs	Vaikimisi täitmata	Õpetaja saab kursusele lisada külalise, kes saab tutvuda kursuse materjalidega ja õppetegevustega aga tema tegevusest ei jää kursusele mingit jälge. Külalise mõte on hea, kui soovid oma kursust avalikkusele näidata, aga ei soovi, et kursust vaatlevad inimesed õppetööd ei segaks.
Kasutaja lisamine kursusele	Vaikimisi täitmata	Saab lisada kursusele kõiki Moodle kasutajaid, muuhulgas lisada teisi õpetajaid või külalisi. Arvestama peab, et külalisena kursusele sisestatud kasutajat teised kursusel osalejad ei näe.
Salasõna	Vaikimisi täitmata	Sead võimaldab piirata kursusele ligipääsetavad külalised vaid nende isikutega, kes teavad ligipääsuks vajalikku salasõna.
Eraldatud rühmad	Vaikimisi täitmata	Õpetaja saab moodustada erinevaid õppijate gruppe ja seadistada neid nii, et grupid näevad omavahel üksteise töid või ei näe. Arvestama peab, et kui õpetaja on kursuse vastavalt seadistanud, siis õpilased ei näe teisi.
Registreerumise võti	Vaikimisi täitmata	Õpetaja saab sisestada kursusele registreerumise salasõna, mille abil

		saavad õpilased ennast kursusele registreerida.

HITSA MOODLE[30]

1.2 eKOOL

ÕPILASE JA LAPSEVANEMA SÄTTED

Säte	Vaikesäte	Kirjeldus ja soovitus
Luban oma isikuandmeid näha: - inimesed minu aadressraamatust - kooli administraatorid ja juhtkond - teised lapsevanemad (koolis) - teised õpilased (koolis) - kõigil eKooli kasutajatel	Vaikimisi: Kooli administraatorid ja juhtkond	Vaikimisi sätet ei saa kasutaja ise eemaldada kuna õpilane ja lapsevanem peavad olema kättesaadavad õpetajatele ja kooli juhtkonnale. Ülejäänud valikud võiksid jääda sisse lülitamata, et vältida oma isikuandmete lekkimist.
Luban oma kontaktinfot (aadress, telefon, e-post) näha: - inimesed minu aadressraamatust - kooli administraatorid ja juhtkond - teised lapsevanemad (koolis) - teised õpilased (koolis) - kõigil eKooli kasutajatel	Vaikimisi: Kooli administraatorid ja juhtkond	Vaikimisi sätet ei saa kasutaja ise eemaldada kuna õpilane ja lapsevanem peavad olema kättesaadavad õpetajatele ja kooli juhtkonnale. Ülejäänud valikud võiksid jääda sisse lülitamata, et vältida oma kontaktandmete lekkimist.
Uudised ja erinevad teated - soovin eKooli internetikeskkonnas näha teateid ja reklaami - palun saatke mulle e-postiga tasuta eKooli uudiskiri	Vaikimisi on kõik kolm valikut aktiivsed	Vaikimisi sätted saab eemaldada. Kui need eemaldad, väldid reklaame ja eKooli uudiskirju.

[30] https://moodle.hitsa.ee/

- palun saatke mulle e-posti teel eKooli partneritele pakkumisi ja teavitus		

eKool[31]

1.3 KAHOOT

KASUTAJA SÄTTED

Säte	Vaikesäte	Kirjeldus ja soovitus
Saada mulle e-kiri kui keegi jagab minuga oma Kahooti mängu	Vaikimisi sisse lülitatud	Vaikimis sätte saab eemaldada. Kui selle eemaldad, ei saa sa teadet selle kohta kui keegi on sinuga mängu jaganud.
Saada mulle e-kiri kui minu mäng on esile tõstetud	Vaikimisi sisse lülitatud	Vaikimis sätte saab eemaldada. Kui selle eemaldad, siis sa ei saa esile tõstmise kohta teavitust.
Muuda oma poolt koostatud mäng avalikuks või privaatseks	Vaikimisi on täidetud säte avalik	Kui soovid mängu muuta privaatseks, muuda sätet vastavalt.

KAHOOT[32]

1.4 FACEBOOK

TURVALISUSE SÄTTED

Säte	Vaikesäte	Kirjeldus ja soovitus
Saa FB teavitus ja e-maili teavitus, kui keegi logib sinu kontole sisse mõnest võõrast seadmest	Vaikimisi on sisse lülitatud valik „Ära saa teavitusi“	Soovituslik on sätted sisse lülitada, sest vastasel korral teavitust ei tule ja sa ei jõua kiirelt reageerida. Kui oled sellise sõnumi saanud ja veendunud et sisseloginu ei ole sina, siis proovi kiirelt ise sisse logida ja muuta parooli. Kui see enam võimalik pole, proovi tellida parooli uuendus, kui ka see enam

[31] https://ee.ekool.eu/index_et.html
[32] https://create.kahoot.it/login

		võimalik pole, siis teavita FB haldureid konto röövimisest.
Kaheastmeline autoriseerimine	Vaikimisi ei ole ühtegi valikut tehtud	Kaheastmeline autoriseerimine raskendab või muudab võimatuks sisselogimise parooli äraarvamise teel. Saad selleks kasutada erinevaid võimalusi. Nt 1) saad tellida oma telefonile smsi teel lisakoodi, mida küsitakse lisaks FB paroolile. 2) usb pulgale salvestatavad koodid, mida saad kasutada lisaks paroolile 3) telefoni laetud rakendus mis genereerib sulle koodi, mida saad kasutada lisaks paroolile 4) koodikaart, selle saad genereerida FBst ja välja printida, seal on toodud hulk ühekordseid koode, mida on mugav kasutada näiteks reisil olles.
Avalik võti	Vaikesätet ei ole määratud	See ei ole reeglina tavakasutajatele mõeldud. Kasutatakse siis, kui sinu arvutis olev rakendus suhtleb ise automaatselt FBga. Siis pead genereerima omale Open PGP standardi järgse krüptovõtme, mille avaliku osa salvestad siia FB sätetesse ja privaatset võtit kasutab sinu rakendus.
Rakenduste salasõnad	Vaikesätet ei ole määratud	Siin saad genereerida omale ühekordsed salasõnad, mida saad kasutada FB kaudu rakendustesse logimiseks. Näiteks saab neid paroole kasutada Xboxi, Spotifysse või Skype logimisel. Selliste paroolide kasutamine kaitseb sind FB paroolide õngitsemise eest, kuna iga parool kehtib ainult ühe korra ja selle teadasaamisel ei saa keegi su kontole ligi.
Tuvastatud seadmed	Vaikesätet ei ole määratud	Kui logid siin nimekirjas olevatest seadmetest FBsse, siis ei saa sa sisselogimisel teavitust - et sisse on logitud võõrast seadmest.

		Kui kasutad FBd näiteks avalikust kohvikust ja lubad sealse seadme oma „usaldatud seadmete“ nimekirja (sulle kuvatakse enne „trusted sites“ teavitus ekraanile. Kui sa sellesse ei süvene ja vajutad „jah“, siis oledki selle avaliku kohviku seadme oma usaldusväärsete seadmete nimekirja lisanud. Kui nüüd keegi sellest seadmest sinu FBsse logib, ei saa sina selle kohta teavitust. Sama kehtib telefonide kohta. Kui sinu mobiiltelefon on lubatud seadmete nimekirjas ja sa kaotad oma telefoni, siis saab telefoni leidja (eeldusel, et ta saab telefoni sisse), sisse ka sinu FB kontole, ilma, et sina selle kohta teavituse saaksid. Seega tuleks siin kuvatavat nimekirja aeg-ajalt üle vaadata ja puhastada (nt kui oled külastanud mõnd avalikku internetipunkti või kaotanud oma telefoni).
Usalduskontaktid	Vaikesätet ei ole määratud	Usalduskontakt on kontakt, kelle saad määrata puhuks, kui sa ühel hetkel ei pääse ise oma kontole enam ligi – nt kas oled unustanud parooli (või on su konto kaaperdatud) ja taastamist oma e-mailile tellida ei saa sest sul pole enam ligipääsu ka oma meilikontole, siis saad usalduskontaktiks määratud sõbra e-postile tellida oma parooli taastamise teate. Usalduskontakt on soovituslik määrata.
Kust olete sisse loginud	Vaikesätet ei ole määratud	Siin saad kontrollida millistest seadmetest oled sisse loginud ja kas need on sinu omad. Kui keegi saab su kontole ligipääsu, ei pruugi ta alati sellest kuidagi märku anda – ta ei postita su ajajoonele midagi, ta ei võta su kontot üle, vaid lihtsalt jälgib su tegevust. Siin saad üle vaadata kehtivad sisselogimise seansid ja

		need vajadusel tühistada. Kindlasti tuleks siis ka vahetada parool, et võõrast seadmest enam sisse logida ei saaks.
Pärandihalduse kontaktisik	Vaikesätet ei ole määratud	Kui sinuga midagi juhtub, saab siin määratud inimene teha su ajajoonele ühe postituse, millega saab teavitada su kontakte juhtunust. Samuti saab ta vastata uutele sõrakutsetele. Teha ei saa tavapostitusi, vaadata sõnumeid, logida sinu kontole, muuta pilte või postitusi, eemaldada kontakte. Pärandihalduse kontaktisik on soovituslik määrata.
Deaktiveeri oma konto	Vaikesätet ei ole määratud	Konto deaktiveerimine muudab sinu profiili kättesaamatuks ja eemaldab su nime ning profiilipildi enamiku asjade juurest, mida oled FBs jaganud. Mõned asjad võivad endiselt teistele nähtavaks jääda, nagu näiteks sinu nimi nende sõbralistis ja sinu poolt saadetud sõnumid.

PRIVAATSUSÄTTED JA TÖÖRIISTAD

Säte	Vaikesäte	Kirjeldus ja soovitus
Kes näevad minu tulevasi postitusi?	Vaikimisi: sõbrad. Valida saad ka: - avalik - sõprade sõrad - välja arvatud need sõbrad - need kindlad sõbrad - ainult mina	Soovi korral saad vaikesätet muuta aga üldiselt on see säte levinuim. Lisaks saab üle vaadata oma vanemate posttuste ligipääsud ja neid vajadusel muuta. Oma postituste privaatsuse taset saad muuta postituse tegemisel. Nii tehtud valiku jätab FB meelde, seega jagatakse sinu kõiki tulevasi postitusi sama publikuga kuni sa seda sätet muudad.
Lisa „Avalik“, kui valik oma jagamissätete valikusse. See säte on ainult alaealistel kasutajatel	Vaikimisi ei ole valik „Avalik“ kuvatud	Kui sa selle valiku teed, siis kuvatakse sinu postituste juures ka valikut „Avalik“ selles listis, kust saad määrata, kellele postitus avaldatakse. See valik võiks olla keelatud.

Kes saavad mulle sõbrataotlusi saata?	Vaikimisi: igaüks. Valida saab ka valiku sõprade sõrad.	Vaikeväärtus on üldiselt turvaline valik, kui sa võõraste sõbrakutseid vastu ei võta. Sätet saab muuta ka kinnisemaks, nii, et sõbrakutseid saavad saata vaid sõprade sõbrad. Ka selle valiku puhul on soovitav võõraid mitte vastu võtta sest viirused levivad ka sõbrakutsete kaudu ja võõrad võivad hakata sulle saatma viirustega linke vms.
Kes saavad mind e-posti järgi otsida?	Vaikimisi: igaüks. Valida saab ka: - igaüks - sõprade sõbrad - sõbrad	Kasutaja privaatsuse kaitsmiseks. Valik, kas soovid, et sind leitakse e-posti aadressi järgi või mitte.
Kes saavad mind telefoninumbri järgi otsida?	Vaikimisi: igaüks. Valida saab ka: - igaüks - sõprade sõbrad sõbrad	Kasutaja privaatsuse kaitsmiseks. Valik, kas soovid, et sind leitakse telefoninumbri järgi või mitte.
Kas lubad FB välistel otsingumootoritel leida infot sinu FB konto kohta?	Alaealistel vaikimisi välja lülitatud. Täiskasvanutel vaikimisi sisse lülitatud	Kui säte on välja lülitatud, siis ei leia üldised otsingumootorid (nt Google) sinu FB konto kohta infot. Kui see säte pole sul olnud konto loomise hetkest alates välja lülitatud ja muudad sätet vanal kontol, siis pead arvestama mõningase viivitusega, et kõikide otsingumootorite lehed jõuaksid selle info uuendada. Alaealistel on vaikesättena märgitud valik „aktiveeri, kui ma saan 18“. Täiskasvanutel on see säte vaikimisi sisse lülitatud – st otsingumootorid leiavad üles info FB konto kohta.

AJAJOONE JA MÄRKIMISTE SÄTTED

Säte	Vaikesäte	Kirjeldus ja soovitus
Kes saab minu ajajoonele postitusi teha?	Vaikimisi: sõbrad. Valida saab ka ainult iseendale	Sätet on võimalik ka kinni keerata sõprade eest ja jätta avatuks ainult endale. See oleks turvaline valik, sest sõprade postituste kaudu võib su ajajoonele sattuda midagi, mida sa ei soovi seal näha.
Kinnita sõprade poolt sinu märkimised	Vaikimisi: keelatud. Valida saab ka lubatud.	Kui mõni sõber märgib (tagib) sind oma postitustes, siis juhul, kui see säte on sisse lülitatud, ei ilmu viide

(tagimised) enne kui need ilmuvad ajajoonele		sinu kohta enne postituse juures nähtavale, kui sa ei ole seda ise lubanud. Selle sätte eesti keelne tõlge on veidi segadust tekitav. Säte on sisse lülitatud, kui oled teinud valiku „Lubatud“ (enable). Ehk, et lubatud on see, et märkimise puhul saad sa selle enne lubamist üle kontrollida.
Kes näeb postitusi kuhu mind märgitud on?	Vaikimisi: sõbrad Igaüks/sõprade sõbrad/sõbrad/ainult mina/kohandatud	Vaikesäte on piisavalt turvaline kui oled sõbraks valinud vaid omale tuttavad ja heatahtlikud inimesed. Sätet saab muuta ka kinnisemaks aga ka avatumaks sõprade sõpradele või kõigile FB kasutajatele.
Kes näeb seda, mida teised on su ajajoonele postitanud?	Vaikimisi: sõbrad Igaüks/sõprade sõbrad/sõbrad/ainult mina/kohandatud	Vaikesäte on sobiv, kui oled sõbraks valinud vaid omale tuttavad ja heatahtlikud inimesed. Sätet saab muuta ka kinnisemaks aga ka avatumaks sõprade sõpradele või kõigile FB kasutajatele.
Vaata üle märked, mida sõbrad sinu postitustele lisavad, enne, kui need Facebookis ilmuvad	Vaikimisi: keelatud. Valida saab ka lubatud.	Kui säte on sisse lülitatud – ehk võimalus on keelatud, siis ei saa sõber ennast sinu ajajoonel märkida (tagida) enne, kui sa pole seda lubanud.
Kui oled postituses märgitud, keda soovid selle lugejaskonda lisada, kui nad sinna veel ei kuulu?	Vaikimisi: Sõbrad . Valida saab veel ainult mina või kohandatud	Kui sind on kellegi postituses märgitud (tagitud), siis saad selle sättega määrata, kes veel saavad selliseid postitusi näha. Vaikesäte on sobiv valik.

BLOKEERIMISE SÄTTED

Säte	Vaikesäte	Kirjeldus ja soovitus
Piiratud nimekiri	Vaikimisi ei ole midagi määratud	Inimene, kelle sa lisad piiratud nimekirja ei näe enam sinu postitusi mida jagad sõpradega. Näevad sinu avalikke postitusi ja sinu sõprade postitusi teie ühiste tuttavate kaudu. Kui sa oled kellegi siia nimekirja lisanud, siis selle kohta FB temale teavitust ei saada. Siia võib lisada näiteks kasutajad, kes ei ole sinu suhtes heatahtlikud ja kommenteerivad su postitusi halvustavalt.

Blokeeri kasutajad	Vaikimisi ei ole midagi määratud	Blokeeritud inimest listi lisatud kasutaja ei saa enam sinu ajajoonele midagi postitada, ei saa sulle sõnumeid saata ega üritustele kutsuda, ega ka sõbrakutset saata. Siia on mõistlik lisada kasutaja kes lisake eelmisele piiratud nimekirja sattunud isikutele näiteks saadab sulle ka ebameeldiva sisuga sõnumeid
Blokeeri sõnumid	Vaikimisi ei ole midagi määratud	Kui sa blokeerid kelleltki tulevad sõnumid või videokõned, siis ei saa need kasutajad enam sinuga ühendust võtta ka FB Messengeri api kaudu. See ei tähenda, et ta ei saa sind enam märkida (tagida) postitustes või näha su postitusi. Siia võid sisestada kasutaja kes sulle ebameeldiva sisuga sõnumeid saadab kuid muul moel su privaatsust ei häiri.
Blokeeri rakenduste kutsed	Vaikimisi ei ole midagi määratud	Kui kellegi rakenduste kutsed blokeerid, ignoreerid selle isiku kõiki tulevasi rakenduste kutseid. Et konkreetse sõbra kutseid blokeerida, kliki "Ignoreeri selle sõbra kõiki kutseid". Siia võid lisada kasutajad, kes saadavad sulle häirivalt palju erinevaid rakenduste kutseid.
Blokeeri ürituse kutseid	Vaikimisi ei ole midagi määratud	Kui blokeerid ürituste kutsed teatud isikult, ignoreerid automaatselt kõiki tulevasi ürituste kutseid sellelt sõbralt. Siia võid lisada sõbrad, kelle ürituste kutseid sa saada ei soovi.
Blokeeri rakendusi	Vaikimisi ei ole midagi määratud	Siia saad määrata rakendused, millele sa ei soovi enam oma infot avaldada. Kui olete varem sellele rakendusele avaldanud oma e-posti aadressi siis saab see rakendus sulle jätkuvalt kirju saata. Kui sa ka neid enam ei soovi, siis pead vajutama nende kirjade all olevatele „eemalda mind kirjasaajate listist“ lingile.
Blokeeri lehti	Vaikimisi ei ole midagi määratud	Kui blokeerid Lehekülje, ei saa see Leht enam sinu postitustega suhelda, sinu postitustele vastata või neid meeldivaks lisada. Sa ei saa enam selle Lehekülje ajajoonele postitada ega Leheküljele sõnumeid saata. Kui oled hetkel Lehekülje meeldivaks lisanud, eemaldab blokeerimine selle

		meeldivate ja jälgitavate hulgast.

AVALIKE POSTITUSTE SÄTTED

Säte	Vaikesäte	Kirjeldus ja soovitus
Kes saavad mind jälgida?	Vaikimisi: Sõbrad. Võimalik valida ka Avalik	Su sõbralisti liikmed näevad su postitusi vaikimisi, samas saad iga uue postituse juures sätet muuta nii, et see postitus oleks avalik.
Kes saavad kommenteerida sinu avalikke postitusi?	Vaikimisi: Sõbrad. Võimalik valida ka Avalik ja Sõprade sõbrad.	Sinu avalikke postitusi saavad kommenteerida need inimesed, kelle oled siit sättest valinud – kas sõbrad, sõprade sõbrad või kõik FB kasutajad. Vaikesäte on sobiv valik.
Avalike postituste teavitused	Vaikimisi: Avalik Võimalik valida veel ka Sõprade sõbrad ja Mitte keegi	Saad määrata kas sa saad teavitusi kui keegi mitte sõpradest hakkab sind jälgima või jagab, märgib meldivaks või kommenteerib su avalikke postitusi. Vaikesäte on sobiv.
Avalik profiili info	Vaikimisi: Sõbrad. Võimalik valida veel ka Avalik ja Sõprade sõbrad	Selle sättega saad määrata milline grupp inimesi saab sinu avalikku profiili pilti ja muud profiili infot meeldivaks märkida või neid kommenteerida. Vaikesäte on sobiv.
Kommentaaride pingerida	Vaikesäte: Väljas. Võimalik valida ka Sees.	Kui kommentaaride pingerida on sisse lülitatud, näed oma avalike postituste juures kõige olulisemaid kommentaare kõige esimesena. Sätte sisse lülitamine ei ole tavakasutajal oluline. Võib olla oluline avaliku elu tegelaste kontodel, kelle postitused saavad väga palju kommentaare.
Kasutajanimi	Vaikesätet pole määratud.	Sa saad oma kasutajanime muuta kuid selle muutmisel määra selline kasutajanimi, mille järgi su sõbrad sind ka edaspidi ära tunnevad.
Twitter		Kui sul on Twitteri konto, siis saad selle sätte alt mugavalt ühendada FBga. Siis saavad su Twitteri sõbrad jälgida su FB postitusi ja vastupidi.

RAKENDUSTE SÄTTED

Säte	Vaikesäte	Kirjeldus ja soovitus
Rakendused, kuhu oled sisse loginud FBga	Kuvatakse rakenduste nimekiri	Siin saad näha millistele rakendustele oled lubanud ligipääsu oma andmetele ja seda vajadusel muuta.
Rakenduse nähtavus	Vaikimisi: Ainult	Selle sättega saad määrata kes

	mina. Valida saab veel: Avalik, Sõbrad, Kohandatud	näevad, et sa seda rakendust kasutada. Vaikesäte on sobiv valik.
Info, mida sellele rakendusele annad	Siin kuvatakse iga rakenduse kohta see info mida rakendus nõuab	Saad otsustada, kas sa kasutad rakendust või mitte. Kui sa ei soovi rakendusele oma infot anda, siis saad selle rakenduse oma loetelust kustutada või rakenduse sätete alt piirata, mida sa soovid sellele näidata ja mida mitte.
Rakendused, veebilehed ja pluginad	Vaikimisi: sisse lülitatud. Saab valida ka: välja lülitatud	Lubab sul kasutada rakendusi, pluginaid, mänge ja veebilehti. Kui säte välja lülitada, siis ei saa sa enam rakendustesse läbi FB sisse logida, sõbrad ei saa sinuga läbi rakenduste ühendust võtta, rakenduste postitused eemaldatakse sinu ajajoonelt. Üldiselt on vaikesäte sobiv valik. Kui aga rakenduste info hakkab häirima, võib sätte välja lülitada.
Mängude ja rakenduste teavitused	Vaikimisi: Sisse lülitatud. Võimalik ka: välja lülitatud.	See säte kontrollib mängude kutseid, mängude uuendamise ja staatuste infot. Sätte väljalülitamine ei takista sul mänge mängida, keelad vaid nende teavitused. Liigse info kuvamise mõttes on soovituslik säte välja lülitada
Teiste kasutatavad rakendused	Vaikimisi on sisse lülitatud valikud: - sugu - minu postitused - sünnipäev - pere ja suhted - haridus ja töö - tegevusalad, huvid - minu veebileht - minu rakenduste aktiivsus - kas olen võrgus Lisaks saab sisse lülitada valikud: - kodulinn - praegune elukoht - huvitun - usulised ja poliitilised vaated	Kui sinu sõber kasutab rakendusi, saavad need rakendused läbi tema konto ligi ka sinu infole, mis on sinu sätetes valitud. Kui sa ei taha, et sõprade rakendused pääseksid ligi sinu infole, lülita need valikud välja.

Vanemad mobiilse Facebooki versioonid	Vaikimisi: Sõbrad. Valida saab ka: Avalik, Sõprade sõbrad, Sõbrad, Ainult mina, Kohandatud	See säte kontrollib nende postituste privaatsust, mis tehakse vanade mobiilsete FB versioonidega, millel pole olnud võimalust valida, kellele oma postituse avalikuks teed (nt vananenud BlackBerry versioon). Vaikesäte on sobiv valik.

FACEBOOKI REKLAAMID

Säte	Vaikesäte	Kirjeldus ja soovitus
Minu FB käitumise järgi reklaamide pakkumine	Vaikesäte: Sisselülitatud. Võimalik ka: Väljalülitatud	Selle sättega saab FBl lubada hinnata oma käitumist FBs ja selle järgi teha endale personaalsemaid pakkumisi reklaamide alal. Kui säte välja lülitada, ei tähenda see, et reklaame enam üldse ei näeks, vaid siis näed suvalisi reklaame. Säte on pigem soovituslik hoida sisselülitatuna, kuid, kui soovid näha ka sind mittehuvitavaid reklaame, siis lülita säte välja.
Minu FB käitumise järgi reklaamide pakkumine ka teistes rakendustes	Vaikesäte: Sisselülitatud. Võimalik ka: Väljalülitatud	Selle sättega saad FBl lubada jagada infot sinu reklaamieelistuste kohta ka teistele rakendustele. Kehtib sama reegel, mis eelmise sätte juures.
Sinu tegevus postituse juures näidatakse postituse kohal jooksvalt välja	Vaikesäte: Ainult minu sõbrad. Võimalik valida ka: Mitte keegi.	Kui märgid midagi meeldivaks, jagad midagi või kommenteerid midagi, siis näidatakse seda postituse juures üleval välja nt „Kati märkis selle hiljuti meeldivaks“ või „Kati hiljuti kommenteeris seda“. Säte on soovitav välja lülitada oma privaatsuse kaitsmise mõttes.
Reklaamieelistuste lisamine		Saad lisada FB poolt kuvatavate reklaamide hulka ka ennast huvitavaid teemasid, neid teemadena ära märkides. Näiteks, kui sind huvitab ujumine, siis võid sinna lisada märksõna „ujumine“, siis kuvatakse sulle reklaamide alale ka ujumisega seonduvaid reklaame. Eelistusi on soovitav info saamise mõttes lisada.

FACEBOOK[33]

33 https://www.facebook.com/

1.5 GOOGLE DRIVE

SISSELOGIMINE JA TURVALISUS

Säte	Vaikesäte	Kirjeldus ja soovitus
Parool ja sisselogimisviis	Vaikesäte puudub	Tugev parool sisaldab segamini numbreid, tähti ja sümboleid. See ei tohiks sarnaneda ühelegi päris sõnale ja seda peaks kasutama ainult Google konto jaoks. Soovitav on lisada kaheastmeline autentimine. Seadistage kas teie telefonile saadetakse ühekordselt kasutatav kood või installeerite telefoni koodide genereerimise rakenduse Autenthicator. Lisaks võite seadistada varuvõimalused, et saaksite sisse logida siis, kui teie teisi samme ei saa kasutada. - ühekordsed prinditavad pääsukoodid võimaldavad sisse logida oma telefonist eemal viibides, näiteks reisimise ajal - hankige oma telefoni Google'i viip ja puudutage sisselogimiseks lihtsalt Jah - turvavõti on väike USB seade, mida kasutatakse sisselogimiseks. Kahekordset autentimist tuleks kindlasti kasutada.
Konto taastevalikud	Vaikesäte puudub	Määrake kindlasti konto taastamise e-posti aadress ja telefoninumber. Kui unustasite parooli või ei pääse kontole juurde, kasutab Google neid sätteid, et teie juurdepääs kontole taastada.
Seadmetoimingud ja märguanded	Vaikesäte puudub	Siin näete 28 viimase päeva turvalisusega seotud tegevusi. Näiteks näete, kui olete muutnud oma parooli või lisanud kontole telefoninumbri. Turvalisuse huvides saate selle alusel

		kontrollida teavet kahtlasest tegevusest.
Viimati kasutatud seadmed	Vaikesäte puudub	Kontrollige, millised seadmed on teie kontole juurde pääsenud ja määrake, kuidas soovite saada hoiatusi, kui Google'i hinnangul on toimumas midagi kahtlast.
Turvahoiatuste sätted	Vaikesäte puudub	Valige, milliseid teavitusi ja kuhu te sooviksite saada. Telli kas teavitus e-postile või sms telefonile.
Ühendatud rakendused ja saidid	Vaikesäte puudub	Vaadake, millistel rakendustel ja saitidel olete lubanud oma kontoga ühenduse luua, ja eemaldage need, mida te rohkem ei usalda.
Slvestatud paroolid	Vaikesäte puudub	Chrome'is ja Androidis kasutatavad paroolid salvestatakse Google Smart Locki ja peetakse kõigis sisse logitud seadmetes teie jaoks meeles. Uute rakenduste ja saitide puhul küsitakse teilt, kas soovite, et Google Smart Lock peaks teie parooli meeles. Google Smart Lock on turvaline lahendus paroolide meelespidamiseks.

ISIKLIK TEAVE JA PRIVAATSUS

Säte	Vaikesäte	Kirjeldus ja soovitus
Teie isiklik teave	Vaikesäte puudub	Hallake oma põhiandmeid, et olla teistele leitav Google'i toodetest Hangouts, Gmail ja Maps, ning muuta teiega ühenduse võtmine lihtsamaks. Muuta saab nime, telefoni, e-maili, aadressi, sünnipäeva, sugu. Seadistada saad ka seda, kas teised näevad sinu sugu ja sünniaastat.
Jagatud soovitused	Vaikesäte puudub	Selleks, et aidata teistel kasutajatel leida veebist lahedaid asju, võidakse teie tegevust (nt arvustusi, lisamisi, jälgimisi, jagamisi jne) kasutada koos teie nime ja fotoga kaubanduslikus või muus reklaamikontekstis. Kui tegemist on jagatud soovitustega reklaamides, saate valida, kas teie nime, fotot ja

		tegevust võib kasutada, et aidata teistel leida asju, mis teile meeldivad (ja vältida asju, mis teile ei meeldi). Kui olete noorem kui 18-aastane, võite näha teiste jagatud soovitusi, kuid teie enda profiilinimi ja -foto ning tegevus ei ilmu jagatud soovitustega reklaamides ja teatud muudes kontekstides.
Blokeeritud kasutajad	Vaikesäte puudub	Blokeerige teisi Google'i kontosid. Blokeerimine on toetatud mõnel, kuid mitte kõikidel Google'i toodetel.
Asukoha jagamine	Vaikesäte puudub	Asukoha jagamine võimaldab teil oma seadmest jagada oma praegust asukohta valitud inimestega. Oma asukoha jagamist teistega võite alustada oma mobiilseadmest
Otsingu sätted	Välja lülitatud	SafeSearch aitab teil Google'i otsingutulemustes blokeerida sobimatud või vulgaarsed kujutised. SafeSearchi filter pole 100% täpne, aga see aitab vältida enamikku vägivaldset ja täiskasvanutele mõeldud sisu. Seega on säte soovtav sisse lülitada.
Otsingu sätted	Kasuta privaatseid tulemusi	Privaatsed tulemused aitavad leida teie jaoks asjakohast sisu, sh sisu ja ühendusi, mida näete ainult teie. Seadistada saab ka valikud: Ära kasuta privaatseid tulemusi. Soovitav on siiski kasutada privaatseid tulemusi.
Otsinguajalugu	Sisse lülitatud	Kui olete sisse logitud, saate asjakohasemaid tulemusi ja soovitusi, mis lähtuvad teie otsingutegevusest. Kui soovite Google eest oma otsinguajalugu varjata, siis on säte soovitav välja lülitada.
Veebi ja rakenduste tegevus	Sisse lülitatud	Paljud Google tooted, nagu Google Now ja Google+ kasutavad teie veebi ja rakenduse tegevust oma soovituste ja värskenduste parendamiseks. Selle seadistuste peatamine piirab

		nende võimet pakkuda teile sellist laadi isikupärastatud sisu. Isegi siis, kui see säte on peatatud, võib Google salvestada ajutiselt otsinguid, et parandada aktiivse otsinguseansi kvaliteeti. Sätte väljalülitamine ei kustuta teie varasemat tegevust. Kui soovite Google eest oma tegevusi varjata ja ei soovi saada isikupärastatud soovitusi, siis on soovitav see säte välja lülitada.
Asukohaajalugu	Sisse lülitatud	Kui selle sätte välja lülitate, ei lisata kohti, kuhu te oma seadmetega lähete, enam teie asukohaajaloo kaardile. See piirab aja jooksul mõnede Google'i toodete, nagu Google Mapsi ja Google Now funktsionaalsust. Kui kasutate selliseid tooteid nagu Otsing ja Maps, võidakse teie privaatse veebi- ja rakenduse tegevuse ühe osana salvestada mõned teie tegevusega seotud asukohaandmed. Asukohaajaloo peatamine ei lülita teie seadme asukoha aruandlust või asukohateenuseid välja. Ajaloo peatamine ei kustuta ka eelnevat tegevust. Kui soovite Google eest oma asukohti varjata, lülitage see säte välja.
Seadme teave	Sisse lülitatud	Sätte väljalülitamine tähendab, et saate tulevaste sündmuste kohta vähem meeldetuletusi ja sellised funktsioonid nagu kõnetuvastus (eriti teie kontaktiloendi nimede puhul) ei pruugi olla enam täpsed. Seadistus ei mõjuta teabe talletamist teatavate teiste Google'i toodete (nagu kalender, kontaktandmed või Play) poolt. Selle sätte peatamine ei kustuta eelnevat sisu. Kui te ei soovi Google poolt sündmuste teavitusi või kõnetuvastust, on soovituslik see sätte välja lülitada.
Hääl- ja helitegevus	Sisse lülitatud	Hääl- ja helitegevuse peatamine võib piirata või keelata funktsioone, näiteks häälotsingu

		alustamist väljendiga „Ok Google“, ja vähendada kõnetuvastuse täpsust Google'i erinevates toodetes, mis kasutavad teie häält. Seadistus ei mõjuta teabe salvestamist teiste Google'i toodete (näiteks Voice) poolt, mida võidakse kasutada teie heli- ja häälsisendite kogumiseks ning talletamiseks. Samuti võib Google jätkata heliandmete kogumist ja salvestamist anonüümselt. Selle seadistuse peatamine ei kustuta varasemat tegevust. Kui te ei kasuta hääle- ja helitegevust, siis on see sätte soovituslik välja lülitada.
Youtube otsinguajalugu	Sisse lülitatud	YouTube'i otsinguajaloo väljalülitamine tähendab, et tulevased otsingud ei kajastu teie otsinguajaloos ja neid ei kasutata paremate soovituste tegemiseks. Sätte väljalülitamine ei kustuta eelnevat tegevust. Kui teie jaoks ei ole Youtube otsinguajalugu oluline talletada, on see säte soovituslik välja lülitada.
YouTube'i vaatamiste ajalugu	Sisse lülitatud	YouTube'i vaatamiste ajaloo väljalülitamine võib muuta teie vaadatud videote otsimise raskemaks ja võib tähendada üle Google'i vähem uute videote soovitusi. Ajaloo peatamine ei kustuta eelnevat tegevust. Kui te ei pea oluliseks Youtube vaatamiste ajaloo salvestamist, siis on soovituslik see säte välja lülitada.
Reklaamide sätted	Sisse lülitatud	Kui lülitate reklaamide isikupärastamise välja näete endiselt reklaame, kuid need on teile vähem kasulikud; teil ei ole enam võimalik osa reklaame blokeerida või summutada; teie nähtavad reklaamid võivad olla seotud vaadatava veebilehe teemaga; teie reklaamisätetesse salvestatud

		teemad eemaldatakse. Kui te ei pea oluliseks isikupärastatud reklaami, siis on sätte väljalülitamine soovituslik.
Reklaamide sätted	Vaikesäte puudub	Eemaldage ebameeldivad teemad ja lisage need, mis teile meeldivad, et muuta teile nähtavad reklaamid teile kasulikumaks. Teemasid lisatakse juurde ka mõne Google'i teenuse kasutamisel (näiteks YouTube'ist videot vaadates).
Hallake oma sisu	Vaikesäte puudub	Teie juhite oma Google'i konto sisu isegi siis, kui lõpetate Google'i toodete kasutamise või otsustate oma konto täielikult kustutada. Kopeerige ükskõik millal oma konto sisu kasutamiseks mõnes teises teenuses või kontol või laadige oma andmed alla. Soovituslik siis, kui soovite Google konto kustutada.
Määrake konto usaldusisik	Vaikesäte puudub	Kinnitage pereliige või sõber, kes osa teie konto sisust alla laadib, kui konto jääb teie määratud ajaperioodiks tähelepanuta. Pärast teie määratud aegumisperioodi käsitletakse kontot passiivsena. Aegumisperiood algab viimasest Google'i kontole sisselogimisest. Passiivse konto automaathaldur teavitab teid enne aegumisperioodi lõppu tekstsõnumi või meili (valikuline) teel. Usaldusväärne kontaktisik on soovituslik lisada.
Konto kustutamine	Vaikesäte puudub	Soovi korral andke Google'ile korraldus oma konto kustutamiseks.

GOOGLE[34]

[34] https://myaccount.google.com/

Lisa 2 Küsitlusankeet

Rolli valik ja haridusasutuse nimetamine

Palun vali roll, kellena küsimustikku täidad ja nimeta kool, kus õpid või töötad. Ma ei võrdle koolide vastuseid omavahel ega too välja vastuseid koolide kaupa, kuid vajan üldinfot mitmest erinevast koolist kokku vastati.

Vali, mis rollis küsimustikku täidad*

- Koolijuht
- Haridustehnoloog või haridustehnoloogi ülesandeid täitev isik
- Õpetaja
- Gümnaasiumi õpilane (10.-12.klass)
- Põhikooli õpilane (7.-9.klass)

Nimeta haridusasutus, kus õpid või töötad*

Õpilane

Klass *

- 7
- 8
- 9
- 10
- 11
- 12

Üldine e-õppe kasutus koolis

1. Milliseks hindad oma digipädevusi arvuti ja nutiseadmete kasutamisel?*
   - Halvaks
   - Pigem halvaks
   - Keskmiseks
   - Pigem heaks
   - Heaks
   - Muu:

2. Milliseks hindad oma õpetajate pädevusi e-õppe kasutamisel?*
   - Halvaks
   - Pigem halvaks
   - Keskmiseks
   - Pigem heaks
   - Heaks

Muu:

3. Milliseid e-keskkondi kasutatakse teie koolis? Nimeta kõik, mida kasutanud oled (nt Moodle, Facebook, Õpiveeb, Edmodo, isiklik blogi, Google Sites, vms)*

4. Järjesta enamkasutatavuse järjekorras - milliseid seadmeid kasutatakse e-õppes kõige enam, keskmiselt, kõige vähem: A-Arvutiklassi arvuteid; B-Kooli süle- või tahvelarvuteid; C-Õpilaste isiklikke vahendeid*

5. Kuidas hindad e-keskkondade kasutuse mahtu teie koolis?*

Väheseks
Pigem väheseks
Piisavaks
Pigem paljuks
Liiga paljuks
Muu:

6. Kui tihti kasutatakse õppetöös e-keskkondi?*

Kord kuus
Kord nädalas
Nädalas mõned korrad
Iga päev
Iga tund
Muu:

7. Kui tihti kasutatakse õppetöös sotsiaalmeediat?*

Kord kuus
Kord nädalas
Nädalas mõned korrad
Iga päev
Iga tund
Muu:

8. Kui õpetaja palub luua e-keskkonda konto, siis luuakse see üheskoos klassis?*

Ei
Pigem ei
Ei tea
Pigem jah
Jah
Muu:

9. Kui õpetaja palub luua e-keskkonda konto, siis annab ta teile juba valmis kasutajanimed ja paroolid?*

Ei

Pigem ei
Ei tea
Pigem jah
Jah
Muu:

10. Kui õpetaja palub luua e-keskkonda konto, siis peab iga õpilane selle loomisega ise hakkama nt kodutööna?*

Ei
Pigem ei
Ei tea
Pigem jah
Jah
Muu:

11. Kas koolis kasutatavad e-keskkonnad võiksid sinu arvates olla:*

Avatud (kõik, kes keskkonda sisenevad, saavad lugeda ülesandeid ja tehtud töid)
Suletud, kuid avatud grupile (keskkonda saab siseneda parooliga ja sisestatud infot näevad vaid grupi liikmed)
Kinnised (keskkond võimaldab teha ülesandeid nii, et vastuseid näeb ainult õpetaja)
Vastavalt vajadusele võiks kasutada erinevaid keskkondi kombineeritult
Muu:

12. Kuidas eelistaksid e-õpet kasutada?*

Keskkondi võiks kasutada koolis tundide ajal
E-õpe on kasutusel ainult kodutöödes
E-õpe on kasutusel osaliselt (nt pooled tunnid on e-õppes ja pooled kontakttundidena)
E-õpe on kasutusel täies mahus, kontakttunde ei toimu
Muu:

Turvateadlikkus ja suhtumine

13. Kas nõustud väitega, et keskkondade turva- ja privaatsussätted on olulised *

Ei
Pigem ei
Enam-vähem
Pigem jah
Jah

14. Kui vastasid “Pigem jah” või “Jah”, siis märgi miks sinu arvates need sätted on olulised:

Saan teada, kas peale minu on veel kellelgi ligipääs minu andmetele (nt

isikuandmetele, hinnetele, üleslaetud töödele)
Kas saan materjalidele ligi ka ilma internetiühenduseta (offline töötamise võimalus)
Kas (ja mis aja jooksul) mul on pärast keskkonnast lahkumist sealt oma (või õpetaja) materjale kätte saada (alla laadida)
Kes vastutab, kui keskkond suletakse ja ma ei saa enam oma materjale kätte
Muu:

15. Kas tutvud enne uue keskkonna kasutuselevõttu selle turvalisuse ja privaatsuse sätetega?*

Ei
Pigem ei
Mõni kord
Pigem jah
Jah
Muu:

16. Kui vastasid "Ei" või "Pigem ei", siis märgi peamised põhjused, miks sa turva- ja privaatsussätetega ei tutvu:

Kuna nii paljud kasutavad seda keskkonda, siis ei saa siin midagi mulle mittesobivat olla
Mul on seda keskkonda vaja kasutada, ma ei saa lähtuda turva- või privaatsussätetest
Mul ei ole selleks aega, need on tavaliselt liiga pikad ja keerulised
Need on sageli inglise keelsed ja ma ei saa nendest aru
Muu

17. Kas oled teadlik erinevatest ohtudest, mis võivad erinevates keskkondades, turva- ja privaatsussätteid eirates või neid mitte teades, ette tulla?*

Ei
Pigem ei
Nii ja naa
Pigem jah
Jah

18. Kui vastasid "Pigem jah" või "Jah", siis märgi peamised allikad, mille abil oled teadlikuks saanud:

Õpetaja (muu kooli töötaja) on koolis rääkinud
Ema - isa (teised lähedased) on kodus rääkinud
Sõbrad on rääkinud
Oled ise lugenud
Muu:

19. Kas mõne keskkonna kasutamisel on sul esinenud mingeid turva- või

privaatsusprobleeme?*

Jah
Ei

20. Kui vastasid "Jah", siis palun nimeta keskkond ja kirjelda esinenud probleemi (nt: minu töö oli kõigile nähtav ja see tekitas minus ebamugavust; - mu hinne oli teistele nähtav ja see tekitas minus ebamugavust; - minu tööle antud kommentaar oli teistele nähtav ja see tekitas minus ebamugavust; - keegi on keskkonnast minu töö kustutanud või seda muutnud; - keegi on minu töö keskkonnast alla laadinud, vahetanud minu nime oma nime vastu ja selle koolile esitanud; - olin unustanud oma parooli ja ma ei saanud seda taastada, vaid pidin looma uue konto, sellega seoses ei saa ma eelmise kasutajakonto alla jäänud töid kätte.

Toe Vajadus

21. Kui sul on mure e-keskkondadega, siis tead kelle poole pöörduda?*

Ei
Pigem ei
Nii ja naa
Pigem jah
Jah

22. Kellelt sa kõige meelsamini e-keskkondadega seoses abi küsiksid?*

Õpetaja (või muu kooli töötaja - haridustehnoloog, IT-tugi)
Vanematelt või teistelt täiskasvanud lähedastelt
Klassi- või koolikaaslastelt
Sõbralt
Internetist
Muu:

23. Millist abi oled vajanud ja saanud e-keskkondade kasutamisel koolist?*

Keskkonda konto loomine
Parooli vahetus, kui see on ununenud
Keskkonna kasutamise juhendamine või juhendid algtasemel
Keskkonna lisavõimaluste juhendid või juhendamine
Keskkonna privaatsussätete tutvustamine
Keskkonna muude turvasätete muutmine
Juhendamine keskkondade avatuse ja suletuse kohta (kes millist infot näevad)
Internetis turvalise käitumise juhendamine koolis kasutusel olevate keskkondade osas, sh sotsiaalmeedia kasutamine õppetöös
Keskkonna sulgemine
Muu:

24. Kui oled mõnes küsimuses jäänud abita, siis millises küsimuses?

25. Mis teemadel tunned, et kool võiks veel tuge pakkuda?*

Pakkuda e-ohutuse intsidentide lahendamisel tuge (nt kui oled saanud kahtlase sisuga meili ja ei tea mida sellega teha või on keegi andnud sulle faile mälupulgal, mida sa ei julge oma arvutiga ühendada või on keegi avaldanud sinu kohta mingi info, mille avalikuks olemist sa ei soovi, kuid ei tea kuidas probleemi lahendada jms)

Tutvustada õpilastele e-keskkondade turvalisuse ja privaatsuse sätteid ja tuua näiteid esinenud probleemidest ja nende lahendustest

Pakkuda infot e-keskkondade turvalisuse ja privaatsuse probleemide kohta, mis võivad tekitada õpilastele soovimatut digijälge

Muu:

26. Kas soovid veel midagi infoks lisada?

Õpetaja

Üldine e-õppe kasutus koolis

1. Milliseks hindate oma digipädevusi arvuti ja nutiseadmete kasutamisel?*

Halvaks
Pigem halvaks
Keskmiseks
Pigem heaks
Heaks
Muu:

2. Milliseks hindate oma pädevusi e-õppe kasutamisel?*

Halvaks
Pigem halvaks
Keskmiseks
Pigem heaks
Heaks
Muu:

3. Milliseks hindate oma kooli 7-12 klassi õpilaste digipädevusi arvuti ja nutiseadmete kasutamisel?*

Halvaks
Pigem halvaks
Keskmiseks
Pigem heaks
Heaks
Muu:

4. Milliseks hindate oma kooli 7-12 klassi õpilaste pädevusi e-õppe kasutamisel?*

Halvaks
Pigem halvaks
Keskmiseks
Pigem heaks
Heaks
Muu:

5. Milliseid e-keskkondi kasutate õppetöös? Nimetage kõik, mida kasutanud olete. Näiteks: Moodle, Facebook, Õpiveeb, Edmodo, isiklik blogi, Google Sites, vms*

6. Järjestage enamkasutatavuse järjekorras - milliseid seadmeid kasutatakse e-õppes kõige enam, keskmiselt, kõige vähem: A-Arvutiklassi arvuteid; B-Kooli süle- või tahvelarvuteid; C-Õpilaste isiklikke vahendeid*

7. Kuidas hindate e-keskkondade kasutuse mahtu teie koolis üldiselt?*

Väheseks
Pigem väheseks
Piisavaks
Pigem paljuks
Liiga paljuks

8. Kuidas hindate e-keskkondade kasutuse mahtu oma ainetes?*

Väheseks
Pigem väheseks
Piisavaks
Pigem paljuks
Liiga paljuks

9. Kui tihti kasutate oma ainetes e-keskkondi?*

Ei kasuta üldse
Kord kuus
Kord nädalas
Mõned korrad nädalas
Iga päev
Iga tund
Muu:

10. Kui tihti kasutate õppetöös sotsiaalmeediat?*

Ei kasuta üldse
Kord kuus
Kord nädalas
Mõned korrad nädalas
Iga päev

Iga tund
Muu:

11. Kui palute õpilastel luua e-keskkonda konto, siis teete seda üheskoos klassis?*
Ei
Pigem ei
Mõni kord
Pigem jah
Jah
Muu:

12. Kui palute õpilastel luua e-keskkonda konto, siis teete konto õpilaste eest ise valmis?*
Ei
Pigem ei
Mõni kord
Pigem jah
Jah
Muu:

13. Kui palute õpilastel luua e-keskkonda konto, siis peab õpilane selle loomisega ise hakkama saama nt kodutööna?*
Ei
Pigem ei
Mõni kord
Pigem jah
Jah
Muu:

14. Kas koolis kasutatavad e-keskkonnad võiksid olla pigem:*
Avatud (kõik, kes keskkonda sisenevad, saavad lugeda ülesandeid ja tehtud töid)
Suletud, kuid avatud grupile (keskkonda saab siseneda parooliga ja sisestatud infot näevad vaid grupi liikmed)
Kinnised (keskkond võimaldab teha ülesandeid nii, et vastuseid näeb ainult õpetaja)
Vastavalt vajadusele võiks kasutada erinevaid keskkondi kombineeritult
Muu:

15. Kuidas eelistaksite e-õpet kasutada?*
E-õpe on ainetunnis lisaväärtus, keskkondi võiks kasutada koolis tundide ajal
E-õpe on kasutusel ainult kodutöödes
E-õpe on kasutusel osaliselt (nt pooled tunnid on e-õppes ja pooled kontakttundidena)
E-õpe on kasutusel täies mahus, kontakttunde ei toimu

Muu:

Turvateadlikkus ja suhtumine

16. Kas nõustute väitega, et keskkondade turva- ja privaatsussätted on olulised*

Ei
Pigem ei
Enam-vähem
Pigem jah
Jah

17. Kui vastasite "Pigem jah" või "Jah", siis märkige miks teie arvates need sätted on olulised:

Saan teada, kas ma saan keskkonda seadistada nii, et minu materjalid ja õpilaste poolt esitatavad tööd on nähtavad ainult mulle või jäävad need nähtavaks kõikidele
Kas saan materjalidele ligi ka ilma internetiühenduseta (offline töötamise võimalus)
Kas (ja mis aja jooksul) mul on pärast keskkonnast lahkumist sealt oma (või õpilaste) materjale kätte saada (alla laadida)
Kes vastutab, kui keskkond suletakse ja ma ei saa enam oma materjale kätte
Muu:

18. Kas tutvute tavaliselt enne uue keskkonna kasutuselevõttu selle turvalisuse ja privaatsuse sätetega*

Ei
Pigem ei
Mõni kord
Pigem jah
Jah
Muu:

19. Kui vastasite "Ei" või "Pigem ei", siis märkige peamised põhjused, miks te turva- ja privaatsussätetega ei tutvu:

Kuna nii paljud kasutavad seda keskkonda, siis ei saa siin midagi mulle mittesobivat olla
Mul on seda keskkonda vaja kasutada, ma ei saa lähtuda turva- või privaatsussätetest
Mul ei ole selleks aega, need on tavaliselt liiga pikad ja keerulised
Kui seal oleks midagi olulist, siis haridustehnoloog (või muu kooli turbe eest vastutav isik) tutvustaks mulle neid ise
Muu:

20. Kas olete teadlik erinevatest ohtudest, mis võivad erinevates keskkondades, turva-

ja privaatsussätteid eirates või neid mitte teades, ette tulla?*

Ei
Pigem ei
Nii ja naa
Pigem jah
Jah

21. Kui vastasite "Pigem jah" või "Jah", siis märkige peamised allikad, mille abil olete teadlikuks saanud:

Haridustehnoloog (või muu kooli turbega tegelev töötaja) on rääkinud
Oleme õpetajatega omavahel arutanud
Sõbrad või tuttavad on rääkinud
Olen ise lugenud
Muu:

22. Kas mõne keskkonna kasutamisel on teil esinenud mingeid turva- või privaatsusprobleeme?*

Jah
Ei

23. Kui vastasite "Jah", siis palun nimeta keskkond ja kirjelda esinenud probleemi:

Toe vajadus

24. Kui õpilastel on esinenud probleeme e-keskkondade kasutamisega, siis nad pöörduvad abi saamiseks teie poole?*

Ei
Pigem ei
Mõni kord
Pigem jah
Jah

25. Milliste e-keskkondade kasutamise probleemidega on õpilased teie poole pöördunud?*

Keskkondadesse konto loomine
Parooli vahetus, kui see on ununenud
Keskkonna kasutamine
Keskkonna turva- ja privaatsussätete tutvustamine ja/või muutmine
Keskkondade avatuse ja suletuse teemadel (kes millist infot näevad)
Internetis turvalise käitumise teemadel koolis kasutusel olevate keskkondade osas, sh sotsiaalmeedia kasutamine õppetöös
Keskkonna sulgemine
Muu:

26. Milliste e-keskkondade kasutamise probleemide lahendamisega te pole ise toime tulnud ja olete vajanud teiste abi?*

Keskkondadesse konto loomine
Parooli vahetus, kui see on ununenud
Keskkonna kasutamine
Keskkonna turva- ja privaatsussätete tutvustamine ja/või muutmine
Keskkondade avatuse ja suletuse teemadel (kes millist infot näevad)
Internetis turvalise käitumise teemadel koolis kasutusel olevate keskkondade osas, sh sotsiaalmeedia kasutamine õppetöös
Keskkonna sulgemine
Muu:

27. Kui teil on mure e-keskkondadega, siis teate kelle poole pöörduda?*

Ei
Pigem ei
Nii ja naa
Pigem jah
Jah

28. Kellelt te e-keskkondadega tekkivate küsimuste puhul abi saate või kelle poole suunate õpilase, kui te ise ei oska teda aidata?*

Oma kooli haridustehnoloogilt (või haridustehnoloogi ülesandeid täitvalt isikult)
Oma kooli IT-juhilt (või teiselt IT-töötajalt)
Mõnelt teiselt oma kooli õpetajalt
Mõne teise kooli töötajalt
Sõpradelt - tuttavatelt
Mõnest hariduse võrgustikust
Internetist
Muu:

29. Kui olete mõnes küsimuses, millega olete edasi pöördunud, jäänud abita, siis millises küsimuses?

30. Mis teemadel tunnete, et kool võiks teile või õpilastele tuge pakkuda?*

Juhendada (või anda kirjalikke juhendeid) kuidas ma õpetajana saaksin õpilasi aidata e-ohutuse intsidentide lahendamisel (nt kui õpilane on saanud kahtlase sisuga meili ja ei tea mida sellega teha või on keegi andnud talle faile mälupulgal, mida ta ei julge oma arvutiga ühendada või on keegi avaldanud tema kohta mingi info, mille avalikuks olemist ta ei soovi, kuid ei tea kuidas probleemi lahendada jms)
Juhendada (või anda kirjalikke juhendeid) milliseid turvalisuse või privaatsuse sätteid ma õpetajana uue e-keskkonna kasutuselevõtul peaksin õpilastele tutvustama, et saaksin ka tuua näiteid esinenud probleemidest ja nende

lahendustest
Pakkuda infot e-keskkondade turvalisuse ja privaatsuse probleemide kohta, mis võivad tekitada nii õpilastele kui mulle endale soovimatut digijälge
Muu:

31. Kas soovite veel midagi lisada?

Haridustehnoloog

Üldine e-õppe kasutus koolis

1. Milliseks hindate oma digipädevusi arvuti ja nutiseadmete kasutamisel?*
   Halvaks
   Pigem halvaks
   Keskmiseks
   Pigem heaks
   Heaks
   Muu:

2. Milliseks hindate oma pädevusi e-õppe kasutamisel?*
   Halvaks
   Pigem halvaks
   Keskmiseks
   Pigem heaks
   Heaks
   Muu:

3. Milliseks hindate oma kooli õpetajate digipädevusi arvuti ja nutiseadmete kasutamisel?*
   Halvaks
   Pigem halvaks
   Keskmiseks
   Pigem heaks
   Heaks
   Muu:

4. Milliseks hindate oma kooli õpetajate pädevusi e-õppe kasutamisel?*
   Halvaks
   Pigem halvaks
   Keskmiseks
   Pigem heaks
   Heaks
   Muu:

5. Milliseks hindate oma kooli 7-12 klassi õpilaste digipädevusi arvuti ja nutiseadmete kasutamisel?*

Halvaks
Pigem halvaks
Keskmiseks
Pigem heaks
Heaks
Muu:

6. Milliseks hindate oma kooli 7-12 klassi õpilaste pädevusi e-õppe kasutamisel? *

Halvaks
Pigem halvaks
Keskmiseks
Pigem heaks
Heaks
Muu:

7. Milliseid e-keskkondi teie koolis kasutatakse? Nimetage kõik, mida teate, et õpetajad kasutavad või kasutate ise?*

8. Järjestage enamkasutatavuse järjekorras - milliseid seadmeid kasutatakse e-õppes kõige enam, keskmiselt, kõige vähem: A-Arvutiklassi arvuteid; B-Kooli süle- või tahvelarvuteid; C-Õpilaste isiklikke vahendeid*

9. Kuidas hindate e-keskkondade kasutuse mahtu teie koolis üldiselt?*

Väheseks
Pigem väheseks
Piisavaks
Pigem paljuks
Liiga paljuks

10. Kui tihti kasutatakse õppetöös e-keskkondi?*

Ei kasutata üldse
Kord kuus
Kord nädalas
Mõned korrad nädalas
Iga päev
Iga tund
Muu:

11. Kui tihti kasutatakse õppetöös sotsiaalmeediat?*

Ei kasutata üldse
Kord kuus
Kord nädalas

Mõni kord nädalas
Iga päev
Iga tund
Muu:

12. Kui õpilastel palutakse luua e-keskkonda konto, siis tehakse seda üheskoos klassis õpetaja juhendamisel?*

Ei
Pigem ei
Mõni kord
Pigem jah
Jah
Muu:

13. Kui õpilastel palutakse luua e-keskkonda konto, siis õpetaja teeb konto õpilaste eest ise valmis?*

Ei
Pigem ei
Mõni kord
Pigem jah
Jah
Muu:

14. Kui õpilastel palutakse luua e-keskkonda konto, siis peab õpilane selle loomisega ise hakkama saama nt kodutööna?*

Ei
Pigem ei
Mõni kord
Pigem jah
Jah
Muu:

15. Kas koolis kasutatavad e-keskkonnad võiksid olla teie arvates pigem:*

Avatud (kõik, kes keskkonda sisenevad, saavad lugeda ülesandeid ja tehtud töid)
Suletud, kuid avatud grupile (keskkonda saab siseneda parooliga ja sisestatud infot näevad vaid grupi liikmed)
Kinnised (keskkond võimaldab teha ülesandeid nii, et vastuseid näeb ainult õpetaja)
Vastavalt vajadusele võiks kasutada erinevaid keskkondi kombineeritult

16. Kuidas teie arvates teie koolis võiks e-õpet rakendada?*

E-õpe on ainetunnis lisaväärtus, keskkondi võiks kasutada koolis tundide ajal
E-õpe on kasutusel ainult kodutöödes
E-õpe on kasutusel osaliselt (nt pooled tunnid on e-õppes ja pooled

kontakttundidena)
E-õpe on kasutusel täies mahus, kontakttunde ei toimu
Muu:

Turvateadlikkus ja suhtumine

17. Kas nõustute väitega, et keskkondade turva- ja privaatsussätted on olulised?*

Ei
Pigem ei
Enam-vähem
Pigem jah
Jah

18. Kui vastasite "Pigem jah" või "jah", siis kirjeldage miks teie arvates need sätted on olulised:

Saan teada, kas ma saan keskkonda seadistada nii, et minu materjalid ja õpilaste poolt esitatavad tööd on nähtavad ainult mulle või jäävad need nähtavaks kõikidele
Kas saan materjalidele ligi ka ilma internetiühenduseta (offline töötamise võimalus)
Kas (ja mis aja jooksul) mul on pärast keskkonnast lahkumist sealt oma (või õpilaste) materjale kätte saada (alla laadida)
Kes vastutab, kui keskkond suletakse ja ma ei saa enam oma materjale kätte
Muu:

19. Kas tutvute tavaliselt enne uue keskkonna kasutuselevõttu selle turvalisuse ja privaatsuse sätetega*

Ei
Pigem ei
Mõni kord
Pigem jah
Jah
Muu:

20. Kui vastasite "Ei" või "Pigem ei", siis märkige peamised põhjused, miks te turva- ja privaatsussätetega ei tutvu:

Kuna nii paljud kasutavad seda keskkonda, siis ei saa siin midagi mittesobivat olla
Mul on see keskkond vaja kasutusele võtta, ma ei saa lähtuda turva- või privaatsussätetest
Mul ei ole selleks aega, need on tavaliselt liiga pikad ja keerulised
Kuna keskkonna võtavad kasutusele õpetajad, siis peavad õpetajad ise sätetega tutvuma ja neid õpilastele tutvustama, see pole minu ülesanne
Muu:

21. Kas olete teadlik erinevatest ohtudest, mis võivad erinevates keskkondades, turva- ja privaatsussätteid eirates või neid mitte teades, ette tulla?*

Ei
Pigem ei
Nii ja naa
Pigem jah
Jah

22. Kas mõne keskkonna kasutamisel on teil esinenud mingeid turva- või privaatsusprobleeme?*

Ei
Jah

23. Kui vastasite "Jah", siis palun nimetage keskkond ja kirjeldage esinenud probleemi:

Toe vajadus

24. Kui õpetajatel on esinenud probleeme e-keskkondade kasutamisega, siis nad pöörduvad abi saamiseks teie poole?*

Ei
Pigem ei
Mõni kord
Pigem jah
Jah

25. Milliste e-keskkondade kasutamise probleemidega on õpetajad või õpilased teie poole pöördunud?*

Keskkondadesse konto loomine
Parooli vahetus, kui see on ununenud
Keskkonna kasutamine
Keskkonna turva- ja privaatsussätete tutvustamine ja/või muutmine
Keskkondade avatuse ja suletuse teemadel (kes millist infot näevad)
Internetis turvalise käitumise teemadel koolis kasutusel olevate keskkondade osas, sh sotsiaalmeedia kasutamine õppetöös
Keskkonna sulgemine
Muu:

26. Kas mõnes küsimuses, millega on teie poole pöördutud, olete vastamisega hätta jäänud? Mis küsimuses?*

27. Kas õpetajad on teie poolt soovitatud e-keskkonnad kasutusele võtnud?*

Ei

Pigem ei
Mõni kord
Pigem jah
Jah
Muu:

28. Mis võiks olla põhjuseks, kui õpetaja ei võta soovitatud keskkonda kasutusele?*
Ta ei oska seda kasutada ja ei küsi ka abi
Ta ei ole põhimõtteliselt huvitatud e-õppest ja e-õppe keskkondadest
Ta ei pea keskkonda omale sobivaks funktsionaalsuse tõttu
Talle ei sobi keskkonna turvalisuse- või privaatsuse sätted
Muu:

29. Mis teemadel tunnete, et kool võiks õpetajatele/õpilastele või ka teile tuge pakkuda:*
Juhendada (või anda kirjalikke juhendeid) kuidas saaks õpilasi aidata e-ohutuse intsidentide lahendamisel (nt kui õpilane on saanud kahtlase sisuga meili ja ei tea mida sellega teha või on keegi andnud talle faile mälupulgal, mida ta ei julge oma arvutiga ühendada või on keegi avaldanud tema kohta mingi info, mille avalikuks olemist ta ei soovi, kuid ei tea kuidas probleemi lahendada jms)
Juhendada (või anda kirjalikke juhendeid) milliste turvalisuse või privaatsuse sätetega peaks uue e-keskkonna kasutuselevõtul tutvuma (ja tutvustama õpetajatele/õpilastele). Anda ka näiteid esinenud probleemidest ja nende lahendustest
Pakkuda infot e-keskkondade turvalisuse ja privaatsuse probleemide kohta, mis võivad tekitada nii õpilastele, õpetajatele, kui mulle endale soovimatut digijälge
Muu:

30. Kas soovite veel midagi lisada?

Koolijuht

Üldine e-õppe kasutus koolis

1. Milliseks hindate oma kooli õpetajate digipädevusi arvuti ja nutiseadmete kasutamisel?*
Halvaks
Pigem halvaks
Keskmiseks
Pigem heaks
Heaks
Muu:

2. Milliseks hindate oma kooli õpetajate pädevusi e-õppe kasutamisel?*

Halvaks
Pigem halvaks
Keskmiseks
Pigem heaks
Heaks
Muu:

3. Milliseks hindate oma kooli haridustehnoloogi (või tema ülesandeid täitva isiku) oskuseid toetada õpetajaid e-õppe kasutamisel?*

Halvaks
Pigem halvaks
Keskmiseks
Pigem heaks
Heaks
Muu:

4. Kuidas hindate e-keskkondade kasutuse mahtu teie koolis üldiselt?*

Väheseks
Pigem väheseks
Piisavaks
Pigem paljuks
Liiga paljuks
Muu:

5. Kui õpilastel palutakse luua e-keskkonda konto, siis milline viis selleks oleks kõige parem?*

Konto luuakse koolis üheskoos, haridustehnoloogi juhendamisel
Konto luuakse koolis üheskoos, õpetaja juhendamisel
Õpetaja või haridustehnoloog teevad ise kontod valmis ja jagavad õpilastele kasutajanimed ja paroolid
Õpilased võiksid konto luua iseseisvalt näiteks kodutööna
Muu:

6. Kas koolis kasutatavad e-keskkonnad võiksid olla teie arvates pigem:*

Avatud (kõik, kes keskkonda sisenevad, saavad lugeda ülesandeid ja tehtud töid)
Suletud, kuid avatud grupile (keskkonda saab siseneda parooliga ja sisestatud infot näevad vaid grupi liikmed)
Kinnised (keskkond võimaldab teha ülesandeid nii, et vastuseid näeb ainult õpetaja)
Vastavalt vajadusele võiks kasutada erinevaid keskkondi kombineeritult

7. Kuidas teie koolis võiks e-õpet rakendada?*

E-õpe on ainetunnis lisaväärtus, keskkondi võiks kasutada koolis tundide ajal
E-õpe on kasutusel ainult kodutöödes

E-õpe on kasutusel osaliselt (nt pooled tunnid on e-õppes ja pooled kontakttundidena)
E-õpe on kasutusel täies mahus, kontakttunde ei toimu
Muu:

Turvateadlikkus ja suhtumine

8. Kas nõustute väitega, et keskkondade turva- ja privaatsussätted on olulised?*
Ei
Pigem ei
Nii ja naa
Pigem jah
Jah

9. Kas tutvute tavaliselt enne uue keskkonna kasutuselevõttu selle turvalisuse ja privaatsuse sätetega?*
Ei
Pigem ei
Mõni kord
Pigem jah
Jah
Muu:

10. Kui vastasite "Pigem jah" või "jah", siis märkige peamised põhjused, miks te turva- ja privaatsussätetega ei tutvu:
Kuna nii paljud kasutavad seda keskkonda, siis ei saa siin midagi mittesobivat olla
Mul on see keskkond vaja kasutusele võtta, ma ei saa lähtuda turva- või privaatsussätetest
Mul ei ole selleks aega, need on tavaliselt liiga pikad ja keerulised
Muu:

11. Kas leiate, et koolis uue e-keskkonna kasutuselevõtul peaks haridustehnoloog õpetajatele keskkonna turva- ja privaatsussätteid tutvustama?*
Ei
Jah

12. Kui koolis puudub haridustehnoloog, siis kes peaks turva- ja privaatsussätteid õpetajatele tutvustama?*

13. Kas leiate, et koolis uue e-keskkonna kasutuselevõtul peaks õpilastele keskkonna turva- ja privaatsussätteid tutvustama?*
Ei
Jah

14. Kes peaks teie arvates koolis uue e-keskkonna kasutuselevõtul õpilastele keskkonna turva- ja privaatsussätteid tutvustama: Märkige kõik sobivad.

Haridustehnoloog
Õpetajad
IT-juht (või muu IT-töötaja)
Muu:

15. Kas olete teadlik erinevatest ohtudest, mis võivad erinevates keskkondades, turva- ja privaatsussätteid eirates või neid mitte teades, ette tulla?*

Ei
Pigem ei
Nii ja naa
Pigem jah
Jah

16. Kas mõne keskkonna kasutamisel on teil esinenud mingeid turva- või privaatsusprobleeme?*

Ei
Jah

17. Kui vastasite "Jah", siis palun nimetage keskkond ja kirjeldage esinenud probleemi

Toe vajadus

18. Kui teie kooli õpetajatel või teil endal esineb probleeme e-keskkondade kasutamisega, siis kelle poole te abi saamiseks saate pöörduda?*

19. Kas teil on tulnud juhtkonna tasandil lahendada mõnd keskkondade turvalisuse või privaatsusega ette tulnud probleemi? Millist, palun kirjeldage:*

20. Millistel keskkondade turvalisuse ja privaatsuse teemadel arvate, et kool vajaks nõuandeid, soovitusi või juhendeid?*

Kuidas kool saaks õpilasi aidata e-ohutuse intsidentide lahendamisel (nt kui õpilane on saanud kahtlase sisuga meili ja ei tea mida sellega teha või on keegi andnud talle faile mälupulgal, mida ta ei julge oma arvutiga ühendada või on keegi avaldanud tema kohta mingi info, mille avalikuks olemist ta ei soovi, kuid ei tea kuidas probleemi lahendada jms)
Milliste turvalisuse või privaatsuse sätetega peaks uue e-keskkonna kasutuselevõtul õpetaja/õpilane tutvuma, milliste sätete eiramine või mitte teadlik olemine võib kaasa tuua probleeme ja kuidas neid vältida/lahendada
E-keskkondade turvalisuse ja privaatsuse probleemide kohta, mis võivad tekitada nii õpilastele, õpetajatele, kui kogu koolile soovimatut digijälge
Muu:

21. Kas soovite veel midagi lisada?