

SAAREMAA GÜMNAASIUMI INFOSÜSTEEMI KASUTAMISE KORD JA ISIKUANDMETE TÖÖTLEMISE PÕHIMÕTTED

1. Üldsätted ja õiguslik alus

1.1. Vastutav töötleja

Kord sätestab Saaremaa Gümnaasiumi (edaspidi: kool) infosüsteemide kasutamise ja isikuandmete töötlemise põhimõtted. Saaremaa Gümnaasiumi kui Haridus- ja Teadusministeeriumi hallatava riigiasutuse tegevus on avalik. Tegevuse käigus töötleme isikuandmeid õigusaktidest tulenevate ülesannete täitmiseks.

Vastutav töötleja:

- Nimi: Saaremaa Gümnaasium
- Registrikood: 77001263
- Aadress: Väljaku 8, 93812 Kuressaare, Saaremaa vald
- Telefon: +372 5374 4869
- E-post: info@saaremaa.edu.ee
- Veebileht: <https://www.saaremaa.edu.ee>

Andmekaitespetsialist:

- Nimi: Merle Rekaya
- E-post: merle.rekaya@saaremaa.edu.ee
- Telefon: +372 517 7194

1.2. Õiguslikud alused

Isikuandmete töötlemine toimub järgmiste õigusaktide alusel:

- Euroopa Parlamendi ja nõukogu määrus (EL) 2016/679 (isikuandmete kaitse üldmäärus, GDPR),
- isikuandmete kaitse seadus (IKS),
- põhikooli- ja gümnaasiumiseadus (PGS),
- Eesti Vabariigi haridusseadus (HaS),
- avaliku teabe seadus (AvTS),
- küberturvalisuse seadus (KüTS),
- Eesti infoturbestandard (E-ITS),
- arhiiviseadus.

Isikuandmete töötlemise õiguslikud alused (GDPR artikkel 6 lõige 1):

- Seadusest tulenev kohustus (GDPR artikkel 6 lõige 1, punkt c) – haridusasutuse põhitegevusega seotud töötlemine, mida seadus nõuab (nt õpilasraamatu pidamine, andmete esitamine EHIS-esse).
- Avaliku ülesande täitmine (GDPR artikkel 6 lõige 1, punkt e) – avaliku sektori ülesannete täitmine, mis tuleneb kooli põhimäärusest.

- Nõusolek (GDPR artikkel 6 lõige 1, punkt a) – ainult vabatahtlike tegevuste puhul, kus seadus töötlemist ei nõua (nt fotode ja videote avaldamine sotsiaalmeedias).
- Lepingu täitmine (GDPR artikkel 6 lõige 1, punkt b) – töösuhete ja töölepingutega seotud andmete töötlemine.

1.3. Dokumendi ulatus

Käesolev dokument ei hõlma:

- juriidiliste isikute ja asutuste andmete töötlemist,
- füüsilise isiku andmete töötlemist, kui andmeid töödeldakse seoses tema ametikohustusega,
- isikuandmete töötlemist veebilehtedel, millele kooli veebilehel viidatakse, kuid mida ei haldada kool.

2. Õpilaste isikuandmete töötlemine

2.1. Töötlemise eesmärgid ja alused

Õpilaste isikuandmeid kogutakse ja töödeldakse ulatuses, mis on seadusega ette nähtud ning vajalik õppe- ja kasvatustöö ning koolielu korraldamiseks. Töötlemine toimub seadusest tuleneva kohustuse alusel (GDPR artikkel 6 lõige 1 punkt c), mis tähendab, et koolil on seaduslik kohustus neid andmeid töödelda. Õpilastega seotud dokumentatsioonile on seatud juurdepääsupiirang ning neid andmeid kolmandatele isikutele ei avaldata.

Töödeldavad andmekategooriad:

- isikuandmed: nimi, isikukood, sünniaeg, kontaktandmed,
- haridusandmed: hinded, puudumised, õppekava täitmine, tunnistused,
- kontaktandmed: vanemate/eestkostjate kontaktandmed,
- terviseiga seotud andmed (eriliigilised isikuandmed): töötleb ainult kooli tervishoiuteenuse osutaja (kooliõde).

2.2. Nõusolekul põhinev töötlemine

Kuni 18-aastase õpilase andmeid töödeldakse vanema või seadusliku esindaja nõusolekul järgmistel vabatahtlikel eesmärkidel:

- õpilase tunnustamine ja kooli tegevuste kajastamine kooli veebilehel,
- fotode ja videote avaldamine kooli sotsiaalmeedias (Facebook, Instagram, YouTube),
- õpilaspileti foto kasutamine kooli õppe- ja infosüsteemide profiilipildina.

Nõusoleku andmine on vabatahtlik ning nõusoleku võib igal ajal tagasi võtta. Nõusoleku tagasivõtmine ei mõjuta enne tagasivõtmist toimunud töötlemise seaduslikkust.

3. Töötajate isikuandmete töötlemine

3.1. Kandideerimine vabale ametikohale

Tööle kandideerimisel töödeldakse esitatud isikuandmeid, et hinnata kandidaadi sobivust vastavale ametikohale. Vajadusel võib kandidaadi kohta koguda täiendavat teavet avalikest allikatest. Kandidaadil on õigus saadud teabega tutvuda ja esitada omapoolsed selgitused ning vastuväited.

Kool eeldab, et kandideerimisdokumentides esitatud soovitajatele on kandideerija andnud õiguse enda kohta käivatele küsimustele vastamiseks ning soovitajad on nõustunud, et kool nende poole teabe saamiseks pöördub.

Kandideerimise dokumentidega tutvuvad ainult värbamisprotsessis osalevad isikud. Kandidaatide andmed on juurdepääsupiiranguga teave, millele kolmandad isikud saavad juurdepääsu ainult seaduses sätestatud juhtudel.

Kandideerimisdokumendid kustutatakse 6 kuud pärast valituks osutunud kandidaadiga töölepingu sõlmimist.

4. Infosüsteemide kasutamine

4.1. Stuudium (õppeinfosüsteem)

E-õppekeskkond Stuudium on õppe- ja kasvatustöö ning koolielu korraldamiseks. Stuudiumis olevad andmed avaldatakse üksnes õpilastele, kooli töötajatele ja õpilaste vanematele/seaduslikele esindajatele.

Keskkonda sisenemine:

- õpilane: parool, ID-kaart või Smart-ID,
- vanem/eestkostja: parool, ID-kaart või Smart-ID,
- töötaja: ID-kaart, Smart-ID või riistvaraline turvavõti (FIDO2).

Volitatud töötaja: OÜ Koodimasin, registrikood 10728286.

4.2. Microsoft 365 (pilveteenus)

Kool kasutab Microsoft 365 teenuseid (Teams, SharePoint, OneDrive, Outlook) dokumendihalduseks, suhtluseks ja õppetöö korraldamiseks.

Keskkonda sisenemine: kaheastmeline kinnitamine (MFA) kõigile kasutajatele.

Volitatud töötaja: Microsoft Ireland Operations Limited.

Andmete asukoht: Euroopa Liit (EL/EMP piirkond).

4.3. TI-rakendus

Kool on kehtestanud „TI-rakenduse kasutamise korra“, mis kohustab kooli õpetajaid, õpilasi ja töötajaid järgima andmekaitse ja küberturvalisuse reegleid:

- TI-rakendusse ei sisestata ees- ja perekonnanimesid, isikukode, aadresse, kontaktandmeid, hindeid, hinnanguid, terviseandmeid;
- ei laadita üles pilte, videoid või helifaile, mis sisaldavad tuvastatavat teavet.

4.4. Muud kasutatavad infosüsteemid

Riiklikud infosüsteemid, milles kool on volitatud töötaja:

- EHIS – Eesti Hariduse Infosüsteem (õpilaste, pedagoogide, kooli ja õppekava andmed),
- EIS – eksamite infosüsteem ja lõpudokumentide plankide haldus,
- SAIS/sisseastumine.ee – kandidaatide avalduste vastuvõtt.

Tugiteenuste süsteemid:

- toitlustusteenus: P. Dussmann Eesti OÜ;
- õpilaspileti teenus: EÜL/eduid.ee;
- turvafirma (videovalve): Riigi Kinnisvara AS;

- heakorrateenus: Riigi Kinnisvara AS;
- kooliõe teenus: Margarita Sikk FIE.

5. Infosüsteemide kasutajate kohustused

5.1. Üldised kohustused

5.1.1. Kõik kooli infosüsteemide kasutajad on kohustatud:

- hoidma oma kasutajatunnuseid ja paroole konfidentsiaalsena,
- mitte jagama oma kontot teiste isikutega,
- kasutama infosüsteeme ainult tööalastel või õppetööga seotud eesmärkidel,
- teavitama viivitamatult IT-juhti turvaprobleemidest või kahtlastest tegevustest,
- järgima kooli infoturbepoliitikat ja E-ITS nõudeid.

5.2. Paroolide nõuded

5.2.1. Paroolide miinimumnõuded:

- pikkus vähemalt 8 tähemärki,
- sisaldab väike- ja suurtähti, numbreid,
- parool tuleb vahetada vähemalt kord aastas,
- sama parooli ei tohi kasutada mitmes süsteemis.

Eelistatud on mitmikautentimise (MFA) kasutamine kõigis süsteemides, kus see on võimalik.

5.3. E-posti kasutamine

5.3.1. Kooli e-posti kasutamisel tuleb järgida järgmisi reegleid:

- 5.3.1.1 e-posti kasutatakse tööalastel eesmärkidel;
- 5.3.1.2 kahtlaste kirjade ja linkide avamisel olla ettevaatlik (õngitsusrünnakud),
- 5.3.1.3 isikuandmeid sisaldavaid manuseid saata ainult krüpteeritult või turvalise kanaliga,
- 5.3.1.4 töölt lahkumisel antakse juurdepääs postkastile üle vastavalt kokkuleppele.

5.4. Riist- ja tarkvara kasutamine

5.4.1. Kasutaja vastutab tema valduses oleva kooli vara ja teabe eest. Riist- ja tarkvara kasutamisel kehtivad järgmised reeglid:

- 5.4.1.1. kasutajal ei ole lubatud installeerida täiendavat tarkvara tööarvutisse ilma IT-juhi loata, välja arvatud automaatsed tarkvara uuendused,
- 5.4.1.2. kasutajal ei ole lubatud ühendada uut riistvara kooli sisevõrku ega seadmeid sisevõrgus ümber paigutada ilma IT-juhi loata,
- 5.4.1.3. kasutaja kohustub viivitamatult teavitama IT-juhti infotehnoloogiliste seadmetega seotud probleemidest,
- 5.4.1.4. õpilastele õppe-eesmärgil antud seadmeid tuleb kasutada ainult õppetööga seotud tegevusteks.
- 5.4.1.5. Raamatukogus arvel olevaid sülearvuteid ja iPade laenutatakse ja tagastatakse raamatukogu koordinaatori vahendusel. iPadide laenutamiseks on vajalik vormistada üleandmisakt juhiabi juures.
- 5.4.2. Kontoritarkvara makrod ja lisaarendused (VBA skriptid, lingitud arvutustabelid jms) on vaikimisi keelatud. Makrode kasutamine on lubatud ainult IT-juhi kirjalikul nõusolekul, kui see on tööülesannete täitmiseks vältimatult vajalik.
- 5.4.3. Lubatud makrod peavad olema dokumenteeritud (eesmärk, autor, kasutusala) ja testitud enne kasutuselevõttu.

5.5. Andmete talletamine ja varundamine

5.5.1. Andmete talletamisel ja varundamisel kehtivad järgmised reeglid:

- 5.5.1.1. Andmed tuleb salvestada kooli pilvekeskkonda (OneDrive, SharePoint) või võrgukettale, mitte kohalikule kõvakettale.
- 5.5.1.2. Isikuandmeid sisaldavaid faile ei tohi salvestada isiklikesse pilveteenustesse ega jagada väliste teenuste kaudu.
- 5.5.1.3. Kooli andmete varundamise tagab IT-juht vastavalt varundusplaanile.

5.6. Arvutivõrgu kasutamine

- 5.6.1. Kooli arvutivõrgu ja WiFi kasutamisel kehtivad järgmised reeglid:
 - 5.6.1.1. kooli võrku tohib ühendada ainult kooli poolt heakskiidetud seadmeid,
 - 5.6.1.2. väljastpoolt kooli võrku kooli ressurssidele ligipääsuks tuleb kasutada VPN-ühendust,
 - 5.6.1.3. kool võib jälgida kasutajate tegevust kooli seadmetes, süsteemides ja arvutivõrkudes ning vajadusel piirata või tõkestada kasutaja tegevust.

5.7. Kaugtöö ja mobiilseadmed

Kaugtöö tegemisel ja mobiilseadmete kasutamisel kehtivad järgmised reeglid:

- 5.7.1. Kaugtööl tuleb tagada tööandmete ja seadmete kaitse volitamata juurdepääsu eest.
- 5.7.2. Mobiilseadmetes peavad olema aktiveeritud ekraanilukk ja seadme krüpteerimine.
- 5.7.3. Seadme kaotamisest või vargusest tuleb viivitamatult teavitada IT-juhti.

5.8. Mobiilseadmete haldus (MDM)

Kooli mobiilseadmete haldus on korraldatud järgmiselt:

- 5.8.1. **Halduslahendus:** Microsoft Intune (pilvepõhine), mida haldab kooli IT-juht.
- 5.8.2. **Hallatavad seadmed ja operatsioonisüsteemid:** kooli omandis olevad Windows 11 lauaarvutid, sülearvutid ja arvutiklassi seadmed.
- 5.8.3. **Kasutusmudel:** kooli omandis olevad isikustatud seadmed, mis on määratud konkreetsele töötajale või õppeklassile.
- 5.8.4. **Isiklikud seadmed (BYOD):** töötajate ja õpilaste isiklikke mobiilseadmeid Intune'iga ei hallata. Isiklikud seadmed saavad kooli WiFi-ühendust eraldi VLAN-i kaudu.
- 5.8.5. **Rakendatavad turvapoliitikad:**
 - Kettakrüpteerimine (BitLocker), taastevõtmed salvestatakse Active Directory'sse.
 - Seadme vastavuskontroll (Compliance Policy).
 - Tarkvara ja turvaparanduste jaotumine.
- 5.8.6. **Pilveteenuste integratsioon:** Microsoft Entra ID (autentimine, MFA), OneDrive ja SharePoint (andmetalletamine).
- 5.8.7. **Reageerimisajad:** seadmeprobleemidele reageeritakse hiljemalt järgmisel tööpäeval.
- 5.8.8. **Seadmegruppide haldus:** Intune võimaldab seadmeid hallata gruppide kaupa (nt õpetajate arvutid, arvutiklassi seadmed).
- 5.8.9. **Vastavus regulatsioonidele:** mobiilseadmete haldus vastab küberturvalisuse seaduse (KüTS), E-ITS, GDPR ja kooli infoturbepoliitika nõuetele.
- 5.8.10. **Kooskõlastus:** mobiilseadmete halduse põhimõtted on kooskõlastatud IT-juhiga.

5.9. Kooli mobiiltelefonide kasutamine

- 5.9.1. Kooli poolt soetatud mobiiltelefone ja SIM-kaarte kasutatakse tööalaste ülesannete täitmiseks. Mõõdukas isiklik kasutamine on lubatud, kui see ei tekita koolile lisakulu.
- 5.9.2. Kooli mobiiltelefonid ei ole liidetud kooli sisevõrgu ega MDM-lahendusega.
- 5.9.3. Kasutaja on kohustatud:
 - 5.9.3.1. Kaitsma telefoni PIN-koodi, sõrmejälje- või näotuvastusega.
 - 5.9.3.2. Aktiveerima SIM-kaardi PIN-koodi.
 - 5.9.3.3. Mitte jagama telefoni ega SIM-kaardi pääsukoodi teistega.

- 5.9.3.4. Mitte salvestama kooli konfidentsiaalseid andmeid telefoni.
- 5.9.3.5. Teavitama telefoni või SIM-kaardi kaotusest või vargusest viivitamatult IT-juhti, kes korraldab SIM-kaardi sulgemise.
- 5.9.3.6. Välismaal viibides kasutama rändlusteenuseid (*roaming*) kokkuhoidlikult. Andmesideteenuse kasutamine välismaal on lubatud ainult tööalasel vajadusel.
- 5.9.4. Sideteenuste arveid kontrollib juhiabi vähemalt kord kvartalis. Anomaalsete kulude korral teavitatakse kasutajat ja direktorit.
- 5.9.5. Kooli mobiiltelefonide ja SIM-kaartide hoolduse ning asendamise korraldab IT-juht.
- 5.9.6. Töölt lahkumisel tagastatakse kooli mobiiltelefon koos SIM-kaardi ja tarvikutega.

5.10. Irdandmekandjate kasutamine

- 5.10.1. Irdandmekandjateks loetakse USB-mälupulgad, välised kõvakettad, SD-kaardid ja muud eemaldatavad andmekandjad.
- 5.10.2. Irdandmekandjatele on lubatud salvestada ainult tööks vajalikke materjale. Isikuandmeid ja konfidentsiaalseid andmeid tohib irdandmekandjale salvestada ainult erandjuhul ja krüpteeritult.
- 5.10.3. Kooli IT-süsteemidega on keelatud ühendada tundmatut päritolu irdandmekandjaid (nt leitud USB-mälupulgad).
- 5.10.4. Irdandmekandja kaotusest või vargusest tuleb viivitamatult teavitada IT-juhti.
- 5.10.5. Irdandmekandjad, mis sisaldavad kooli andmeid, tuleb enne kasutusest kõrvaldamist turvaliselt kustutada (andmete ülekirjutamine). Füüsiliselt kahjustatud andmekandjad tuleb tagastada IT-juhile hävitamiseks.
- 5.10.6. Irdandmekandjate kasutamise reegleid tutvustatakse töötajatele turvateadlikkuse koolitusel.

5.11. Turvakoolitus

- 5.11.1. Kõik kooli töötajad peavad läbima turvateadlikkuse koolituse vähemalt kord aastas. Uus töötaja kinnitab enne IT-vahendite kasutuselevõttu kirjalikult, et on käesoleva korraga tutvunud.

6. Veebileht ja sotsiaalmeedia

6.1. Veebilehe külastamine

- 6.1.1. Kooli veebilehe külastamisel salvestatakse järgmised andmed:
- 6.1.1.1. IP-aadress (ei seota isikut tuvastava teabega),
- 6.1.1.2. veebilehitseja ja operatsioonisüsteemi versioon,
- 6.1.1.3. külastamise aeg ja külastatud leheküljed.
- Andmeid kasutatakse külastusstatistika tegemiseks veebilehe arendamiseks.

6.2. Küpsised

Kool kasutab järgmisi küpsiseid:

- seansiküpsised (ajutised) – võimaldavad teenuse kasutamist,
- püsiküpsised – jätavad meelde kasutaja valikud,
- analüütilised küpsised (Google Analytics) – külastusstatistika.

Kasutajal on õigus keelduda küpsiste salvestamisest veebilehitseja seadete kaudu. Küpsiste blokeerimisel ei pruugi kõik veebilehe funktsioonid olla kättesaadavad.

6.3. Sotsiaalmeedia

Facebook:

- lehekülg on kõigile nähtav,
- igaüks võib leheküljel postituse avaldada,
- töökeeleks on eesti keel,
- rakendatud on automaatne solvavate väljendite filter (Profanity Filter),
- privaatne suhtlus on võimaldatud.

Instagram:

- lehekülg on kõigile nähtav,
- töökeeleks on eesti keel,
- privaatne suhtlus on võimaldatud,
- märgistamine (*tagimine*) on lubatud.

Kogutud kasutusstatistika andmed saadakse anonüümsel kujul. Täpsemalt saab lugeda Facebooki ja Instagrami andmepoliitikatest.

7. Jälgimisseadmestiku kasutamine (videovalve)

Kooli hoones ja territooriumil on videovalve järgmistel eesmärkidel:

- hoone, territooriumi ja vara kaitseks,
- isikute turvalisust ohustava olukorra ennetamiseks ja olukorrale reageerimiseks,
- korrarikkumise menetlemisel asitõendite väljaselgitamiseks.

Jälgimisseadmestiku haldaja: Riigi Kinnisvara AS.

Juurdepääsuõigus videovalve otsepildile ja salvestistele:

- direktor,
- juhiabi,
- administraator,
- õppenõustaja.

Salvestisi säilitatakse 3 kuud salvestamise päevast arvates. Salvestist säilitatakse elektrooniliselt piiratud juurdepääsuga infosüsteemis ja valvatavas ruumis.

Turvakaamerate salvestisi võib näidata ja väljastada korrakaitseorganitele nende taotluse alusel.

Klassiruumides on keelatud pildistamine ja salvestiste tegemine ilma kohalolijate nõusolekuta. Avalike suurürituste puhul (aktused, konverentsid, võistlused, õppekäigud) on piltide või salvestiste tegemine ja jagamine lubatud vaid korraldaja nõusolekul.

8. Andmete säilitamine

Isikuandmete säilitamise tähtajad:

Andmekategooria	Säilitustähtaeg	Märkused
Õpilaste põhiandmed (õpilasraamat)	alaline	Arhiiviväärtuslik
Õppetulemused (päevikud, tunnistused)	5 aastat	
Lõputunnistused	alaline	
Kandideerimisdokumendid	6 kuud	Pärast konkursi lõppu

Videovalve salvestised	3 kuud	
Veebilehe statistika	26 kuud	Anonüümitud
Kirjavahetus	5 aastat	

Arhiiviväärtuslikud andmed antakse säilitamiseks üle avalikku arhiivi ning üleantud andmete töötlemine lõpetatakse. Arhiiviväärtuseta andmeid töödeldakse säilitustähtaja möödumiseni.

9. Andmesubjekti õigused

9.1. Seoses isikuandmete töötlemisega on andmesubjektil järgmised õigused:

- 9.1.1. õigus tutvuda oma andmetega (GDPR artikkel 15) – saada kinnitust, kas teie kohta andmeid töödeldakse, tutvuda kogutud andmetega ning saada neist koopia;
- 9.1.2. õigus andmete parandamisele (GDPR artikkel 16) – nõuda ebaõigete, ebapiisavate, puudulike või väärade andmete parandamist;
- 9.1.3. õigus andmete kustutamisele (GDPR artikkel 17) – nõuda andmete kustutamist, kui töötlemiseks puudub õiguslik alus või kui andmeid ei ole enam vaja sellel eesmärgil, milleks neid koguti;
- 9.1.4. õigus töötlemise piiramisele (GDPR artikkel 18) – nõuda töötlemise piiramist teatud olukordades, näiteks kui andmete õigsus on vaidlustatud või töötlemine on ebaseaduslik;
- 9.1.5. õigus andmete ülekandmisele (GDPR artikkel 20) – saada oma isikuandmed struktureeritud, üldkasutatavas ja masinloetavas vormingus ning edastada need teisele vastutavale töötlejale. Kui see on tehniliselt teostatav, on andmesubjektil õigus nõuda andmete otseülekandmist ühelt vastutavalt töötlejalt teisele;
- 9.1.6. õigus esitada vastuväiteid (GDPR artikkel 21) – avaliku ülesande täitmise või vastutava töötleja õigustatud huvi alusel toimuva töötlemise vastu.

9.2. Õiguste teostamiseks tuleb esitada allkirjastatud taotlus (sealhulgas digitaalselt allkirjastatud) kooli üldmeilile info@saaremaa.edu.ee või andmekaitse spetsialistile. Taotlusele vastatakse 30 päeva jooksul alates taotluse kättesaamisest. Juhul kui vastamine nõuab pikemat aega taotluse keerukuse või mahu tõttu, võib tähtaega pikendada kuni kahe kuu võrra, teavitades sellest andmesubjekti.

9.3. Kui andmesubjekt leiab, et tema õigusi on rikutud, on tal õigus pöörduda:

- 9.3.1. Andmekaitse Inspeksiooni poole (www.aki.ee);
- 9.3.2. kohtu poole.

10. Turvaintsidentide käsitlemine

10.1. Teavitamine

10.1.1. Turvaintsidentist (sh isikuandmetega seotud rikkumine) tuleb viivitamatult teavitada:

- 10.1.1.1. IT-juhti (olle.arak@saaremaa.edu.ee, tel 512 2169);
- 10.1.1.2. andmekaitse spetsialisti isikuandmetega seotud rikkumiste korral (merle.rekaya@saaremaa.edu.ee).

10.2. Järelevalveasutuste teavitamine

10.2.1. Isikuandmetega seotud rikkumistest teavitatakse:

- 10.2.1.1. Andmekaitse Inspeksiooni 72 tunni jooksul pärast rikkumisest teadasaamist (GDPR artikkel 33);
- 10.2.1.2. andmesubjekte ehk isikuid, kelle andmed lekkisid, kui rikkumine võib põhjustada kõrge riski nende õigustele ja vabadustele (GDPR artikkel 34).

10.2.2. Küberintsidentidest teavitatakse:

10.2.2.1. Riigi Infosüsteemi Ameti CERT-EE-d vastavalt küberturvalisuse seaduse §-le 8 – tõsisemate intsidentide korral, mis ohustavad võrgu- ja infosüsteemide turvalisust.

10.2.3. Kõik isikuandmetega seotud rikkumised tuleb dokumenteerida vastavalt GDPR artikli 33 lõikele 5, sõltumata sellest, kas rikkumisest teavitatakse Andmekaitse Inspeksiooni või mitte. Dokumenteerimine peab hõlmama rikkumise asjaolusid, mõju ja võetud parandusmeetmeid.

11. Infoturbe korraldus S (E-ITS)

Kool rakendab Eesti infoturbestandardit (E-ITS) vastavalt küberturvalisuse seadusele. E-ITS rakendamist koordineerib IT-juht koostöös andmekaitse spetsialistiga.

Infoturbe dokumentatsioon:

- 11.1. infoturvapoliitika – kinnitatud direktori poolt,
- 11.2. infoturbe meetmete rakendusplaan (IMR),
- 11.3. riskianalüüs ja kaitsetarbe hinnangud,
- 11.4. varade register.

E-ITS auditi viimane kuupäev: audit on planeeritud läbi viia 2027. a I kvartalis.

12. Muu info

- 12.1. Kool ei müü, rendi ega üüri teie isiklikke andmeid teistele.
- 12.2. Kool ei jaga teie isiklikke andmeid kolmandate isikutega, välja arvatud juhul, kui seda nõuavad seadused või kui seda on vaja teile õppe- ja kasvatustöö tugiteenuste osutamiseks (nt toitlustus, õpilaspilet, õppeinfosüsteem).
- 12.3. Kool ei edasta veebilehe külastaja andmeid väljapoole Euroopa Majanduspiirkonda.

13. Lõppsätted

- 13.1. Kord jõustub direktori käskkirjaga kinnitamise päeval.
- 13.2. Korra täitmist kontrollib IT-juht koostöös andmekaitse spetsialistiga.
- 13.3. Korda vaadatakse üle vähemalt kord aastas või oluliste muudatuste korral.
- 13.4. Korda tutvustatakse töötajale dokumendihaldussüsteemi Pinal vahendusel. Märkides korra teadmiseks võetuks, kinnitab töötaja, et on korraga tutvunud. Kord on töötajale igal ajal Pinalis kättesaadav.

Kõigi küsimustega, mis on seotud isikuandmete töötlemise ja eelnimetatud õiguste kasutamisega, on võimalik pöörduda:

andmekaitse spetsialist: Merle Rekaya, merle.rekaya@saaremaa.edu.ee,

IT-juht: Olle Arak, olle.arak@saaremaa.edu.ee.