Upplýsingaöryggisstefna Heilsuleikskólans Álfasteins

Heilsuleikskólinn Álfasteinn safnar og viðheldur upplýsingum sem snerta starfsemi leikskólans. Með þessari skjalfestu upplýsingaöryggisstefnu vill leikskólinn leggja áherslu á mikilvægi persónuverndar og upplýsingaöryggis við vinnslu þessara upplýsinga.

Hlutverk þessarar stefnu er að lýsa skuldbindingu *Heilsuleikskólans Álfasteins* til að vernda upplýsingar leikskólans gegn ógnunum, innan frá og utan, vísvitandi og óviljandi. Markmið stjórnunar upplýsingaöryggis er að tryggja áframhaldandi aðgang að upplýsingunum og lágmarka tjón, ef skaði verður, með því að koma í veg fyrir eða lágmarka áhrif af atvikum sem geta truflað vinnslu upplýsinganna eða valdið upplýsingaleka.

Leikskólinn heldur m.a. utan um viðkvæmar persónugreinanlegar upplýsingar sem ber að vernda sérstaklega. Hagsmunir aðila, sem tengjast málum er upplýsingarnar varða, gætu skaðast ef upplýsingarnar komast í rangar hendur, eru rangar eða eru ekki aðgengilegar þegar þeirra er þörf. Þess vegna skilgreinir Álfasteinn þessa öryggisstefnu er varðar trúnað, réttleika og tiltækileika gagna.

Trúnaður. *Heilsuleikskólinn Álfasteinn* tryggir að eingöngu aðilar, sem til þess hafa heimild, hafi aðgang að upplýsingum leikskólans.

Réttleiki gagna. *Heilsuleikskólinn Álfasteinn* tryggir að upplýsingar sem skráðar eru séu réttar og nákvæmar á hverjum tíma.

Tiltækileiki gagna. *Heilsuleikskólinn Álfasteinn* tryggir að skráðar upplýsingar séu aðgengilegar þeim sem hafa heimild og þurfa að nota þær þegar þeirra er þörf. Leikskólinn tryggir einnig að kerfi og gögn sem kunna að eyðileggjast sé hægt að endurreisa með hjálp viðbragsáætlunar og afrita sem geymd eru á öruggum stað.

Öryggisstefna þessi tekur mið af gildandi lögum og reglugerðum um persónuvernd og vinnslu persónuupplýsinga. Öryggisstefnan er í fullu samræmi við reglur Persónuverndar nr. 299/2001 um öryggi persónuupplýsinga og uppfyllir kröfur staðalsins ÍST EN ISO/IEC 27001.

Starfsmenn sem hafa aðgang að upplýsingaverðmætum og þeir vinnsluaðilar, sem koma að rekstri upplýsingakerfa eða vinnslu upplýsinga, skulu hafa aðgang að og þekkja til þessarar öryggisstefnu og þess hluta reglubókar sem snertir þeirra vinnu. Viðurlög komi fram í ráðningarsamningum, starfslýsingum, kjarasamningum eða lögum og felist eftir atvikum í skriflegri áminningu eða brottrekstri.

Hörgársveit 19.06. 2020

Leikskólastjóri, Heilsuleikskólans Álfasteins, Hugrún Ósk Hermannsdóttir

Formaður fræðslunefndar, María Tryggvadóttir

Ítarleg stefna

Markmið og leiðir:
Það er markmið leikskólans að nota raunhæfar, viðeigandi, hagnýtar og árangursríkar öryggisráðstafanir til að vernda mikilvæg verkferli og upplýsingaverðmæti. Sérstaklega skal tryggja að:

- aðgengi að upplýsingaverðmætum sé bundið við þá sem til þess hafa heimild;
- upplýsingar séu varðveittar á tryggilegan hátt;
- farið sé að lögum um leikskóla og persónuvernd varðandi aðgang, vinnslu, flutning, varðveislu og dreifingu upplýsinga;
- haldin sé viðeigandi leynd og trúnaður um upplýsingar;
- réttleiki upplýsingar sé tryggður með því að verja þær fyrir óheimilum breytingum og rangar upplýsingar séu leiðréttar án ónauðsynlegra tafa;
- ákvæði laga, reglugerða og samninga séu uppfyllt;
- útbúin sé viðbragðsáætlun, henni haldið við og hún prófuð eins og kostur er;
- starfsmönnum sé veitt viðeigandi fræðsla og þjálfun varðandi öryggiskröfur tengdar upplýsingum leikskólans;
- tilkynnt sé um öll öryggisatvik og grunaða veikleika á öryggiskröfum og -kerfum og slíkt rannsakað;
- í öryggisreglum sé sérstaklega tekið á vírusavörn og aðgangsstjórnun.

Gildissvið:
1. Öryggisstefna þessi nær til og gildir um alla sem hafa aðgang að upplýsingum leikskólans og upplýsingaverðmætum tengdum þeim. Í henni er skilgreint lágmarksöryggi.

Ábyrgð og skipulag:
1. Leikskólastjóri er endanlega ábyrgur fyrir öryggi upplýsingar sem leikskólinn heldur utan um.
2. Leikskólastjóri skal sjá til þess að starfsfólk sem notar upplýsingar leikskólans hljóti viðeigandi fræðslu um persónuvernd og öryggismál.
3. Leikskólastjóri skal vera tengiliður við forsjáraðila, Persónuvernd og persónuverndarfulltrúa, vegna mála er varða friðhelgi og vernd persónugreinanlegra upplýsinga.
4. Leikskólastjóri er ábyrgur fyrir því að allir hlutaðeigandi starfsmenn leikskólans þekki og skilji öryggisstefnu þessa og hafi hana að leiðarljósi í starfi sínu. Leikskólastjóri getur falið tilteknum starfsmanni daglega framkvæmd þessa þáttar.
5. Það er á ábyrgð sérhvers starfsmanns að fylgja þessari öryggisstefnu og öryggisreglum sem koma fram í reglubók leikskólans.

Endurskoðun, áhættumat og innra eftirlit:
1. Öryggisstefnuna skal endurmeta að minnsta kosti á tveggja ára fresti. Verði veruleg breyting á áhættuþáttum skal endurmeta öryggisstefnuna án tafar.
2. Áhættumat/áhrifamat skal vera viðvarandi og í samræmi við kröfur Persónuverndar. Það skal endurskoðað á minnst tveggja ára fresti og í hvert sinn sem veruleg breyting verður á umhverfi upplýsingavinnslu eða áhættuþáttum.
3. Öryggisþarfir skal greina út frá áhættu-/áhrifamati og greiningu á öryggiskröfum laga og opinberra eftirlitsaðila.
4. Velja skal viðeigandi tæknilegar og skipulagslegar öryggisráðstafanir til að vernda upplýsingar leikskólans. Öryggisráðstafanir skal endurskoða samhliða endurmati á öryggisstefnu og áhættu-/áhrifamati.
5. Beita skal ráðstöfunum sem tryggja nægilegt öryggi með tillit til kostnaðar og í hlutfalli við áhættu sem dregið er úr og hugsanlegt tjón ef öryggisfrávik verða.

6. Viðhafa skal reglubundið innra eftirlit með vinnslu upplýsinga og meðferð upplýsingaverðmæta til að ganga úr skugga um að unnið sé í samræmi við gildandi lög og reglur og þær öryggisráðstafanir sem ákveðnar hafa verið.
7. Tíðni eftirlitsins og umfang þess skal ákveðið með hliðsjón af áhættu, eðli verðmæta sem vernda á, þeirri tækni sem notuð er til að tryggja öryggi þeirra og kostnaði af framkvæmd eftirlitsins. Það skal þó eigi vera gert sjaldnar en árlega.

Aðgangur, notkun og notagildi upplýsinga:

1. Aðgangur starfsmanna að upplýsingum leikskólans er háður tilskyldum heimildum og um hann gilda strangar öryggis- og starfsreglur, sem fram koma í reglubók og tengdum verklagsreglum. Aðgangsheimildum skal stýra tryggilega og skal leikskólastjóri hafa eftirlit með þeim.
2. Um aðgang forsjáraðila að upplýsingum um börn sín gilda strangar öryggisreglur sem nánar eru tilgreindar í reglubók og tengdum verklagsreglum.
3. Aðgangsheimildum að upplýsingum skal ætíð viðhaldið og breytingar á stöðu notenda skulu án tafar tilkynntar til rekstraraðila aðgangsstjórnunar þegar um rafræn kerfi er að ræða.
4. Allur gagnaaðgangur í rafrænum kerfum skal skráður og skilja eftir úttektarslóð sem safnað er í rekstrardagbók kerfisins.
5. Leikskólastjóri skal hafa eftirlit með aðgangi og notkun upplýsinga leikskólans. Skólastjóri getur falið tilteknum starfsmanni daglega framkvæmd þessa þáttar.
6. Beita skal tæknilegum aðgangshindrunum, svo sem eldveggjum, dulkóðun, aðgangsorðum, skjásvæfum og öryggiskerfum,til að fyrirbyggja aðgang óviðkomandi um tölvunet og fjarskiptakerfi sem tengjast eða eru notuð af starfsfólki leikskólans til að tengjast upplýsingum rafrænt og læstum hirslum þegar upplýsingar eru á pappír eða öðrum raunlægum miðlum.

Leynd og réttleiki gagna:

1. Persónuvernd og trúnaður persónuupplýsinga skal tryggður í samræmi við ákvæði laga nr. 90/2018 um persónuvernd og vinnslu persónuupplýsinga, reglna nr. 299/2001 um öryggi persónuupplýsinga og reglugerðar Evrópuþingsins og ráðsins (ESB) nr. 2016/679. Varðandi söfnun, vinnslu, flutning, vörslu og dreifingu persónuupplýsinga skal eftirfarandi að lágmarki virt:
    a. að þær séu unnar með lögmætum, sanngjörnum og gagnsæjum hætti;
    b. að þær séu fengnar í skýrt tilgreindum og lögmætum tilgangi og ekki unnar frekar á annan hátt að ósamrýmanlegt sé þeim tilgangi;
    c. að þær séu nægilegar, viðeigandi og takmarkast við það sem nauðsynlegt er miðað við tilgang vinnslunnar;
    d. að þær séu áreiðanlegar og, ef nauðsyn krefur, uppfærðar, persónuupplýsingar sem eru óáreiðanlegar, miðað við tilgang vinnslu þeirra, skal eytt eða þær leiðréttar; Þó skal hafa í huga ákvæði laga um opinber skjalasöfn;
    e. að þær séu varðveittar á því formi að ekki sé unnt að persónugreina skráða einstaklinga lengur en þörf krefur miðað við tilgang vinnslu;
    f. að þær séu unnar með þeim hætti að viðeigandi öryggis persónuupplýsinga sé tryggt;
    g. að skólinn geti sýnt fram á hann hlíti lögum og reglum sem gilda um vinnsluna;
    h. að til staðar séu viðeigandi tæknilegar og stjórnunarlegar aðgerðir til að verja réttindi hins skráða;
    i. að hinum skráða/forsjáraðilum sé gerð grein fyrir rétti sínu til að vita hvaða upplýsingar eru skráðar og fá rangar upplýsingar leiðréttar;
    j. að upplýsingum um hinn skráða sé þá aðeins deilt með þriðja aðila, að fyrir liggi samþykki hins skráða/forsjáraðila eða að miðlun þeirra styðjist við heimild í lögum;

k. að hinn skráði/forsjáraðilar séu upplýstir án ónauðsynlegra tafa hafi upplýsingarnar borist í hendur óviðkomandi aðila, s.s. vegna gagnaleka. Jafnframt skal slíkur leki tilkynntur til Persónuverndar innan 72 stunda.

2. Allar upplýsingar sem skráðar eru í upplýsingakerfi skulu vera skráðar rétt og á nákvæman hátt miðað við upplýsingagjöf.
3. Viðkvæm gögn með hátt trúnaðarstig skal ekki senda um ytri nettengingar nema þau séu tryggilega varin fyrir hnýsni, t.d. með dulkóðun eða lokuðum samskiptarásum.
4. Setja skal upp varnir gegn spilliforritum til að tryggja leynd, réttleika og aðgengileika gagna.
5. Starfsmenn skulu undirrita yfirlýsingum um að halda trúnað um upplýsingar, sem þeir verða áskynja í starfi sínu. Auk þess skulu þeir undirrita yfirlýsingu um að virða þær reglur um öryggi sem birtast í þessari öryggisstefnu og reglubók leikskólans.

Neyðarstjórnun og öryggisfrávik:

1. Tryggja skal samfelldan rekstur upplýsingakerfa leikskólans í samræmi við niðurstöðu áhættumats/áhrifamats.
2. Öll frávik frá öryggisstefnu skal tilkynna til viðeigandi aðila.
3. Atriði sem varða brot á lögum skulu tilkynnt hlutaðeigandi yfirvöldum.

Reglubók:

1. Útbúin skal reglubók vegna vinnslu persónugreinanlegra upplýsinga hjá leikskólanum með skriflegum verklagsreglum um útfærslu öryggisstefnunnar.
2. Í reglubókinni skal að lágmarki vera:
   - upplýsingar um leikskólann og viðeigandi öryggisþarfir;
   - rammi öryggisstjórnunar, þ.e. hvernig öryggismálum er stjórnað; verksvið vegna tilsjónar með persónuvernd, trúnaðaryfirlýsing, fræðsla um kerfið og fl.;
   - lýsing á upplýsingaöryggiskerfi;
   - lýsing á þeim aðferðum sem notaðar eru við áhættumat/áhrifamat;
   - yfirlit yfir eftirlitsaðgerðir og varúðarráðstafanir sem hrint hefur verið í framkvæmd.
3. Reglubókin skal studd viðeigandi verklagsreglum.
4. Reglubókina skal yfirfara og endurskoða reglulega, minnst á tveggja ára fresti.
5. Efni reglubókar skal vera gert aðgengilegt í samræmi við þarfir hvers og eins.

Staðlar, lög og reglugerðir:

1. Leikskólinn skal uppfylla gildandi lög og reglugerðir sem lúta að vinnslu persónugreinanlegra upplýsinga.
2. Öryggisstefna og öryggisreglur eru mótaðar í samræmi við alþjóðlega viðurkennda staðla, m.a. útgefna af Staðlaráði Íslands, Alþjóðastaðlastofnuninni (ISO) og Evrópsku staðlastofnuninni (IEC).