Upplýsingaöryggisstefna nemendaskrár *Blönduskóla*

Blönduskóli viðheldur nemendaskrá til að halda utan um upplýsingar um nemendur sína, námsframvindu og annað sem nauðsynlegt er vegna náms þeirra við skólann. Með þessari skjalfestu upplýsingaöryggisstefnu vill Blönduskóli leggja áherslu á mikilvægi persónuverndar við vinnslu nemendaskrár skólans.

Blönduskóli hagnýtir m.a. upplýsingatækni til að varðveita gögn nemendaskrár og miðla þeim á öruggan og hagkvæman hátt. Það auðveldar skólanum, nemendum og forsjármönnum nemenda að hafa yfirsýn yfir skráningar, utanumhald, námsframvindu nemenda og árangur í skólastarfi.

Hlutverk þessarar stefnu er að lýsa skuldbindingu Blönduskóla að vernda nemendaskrána gegn ógnunum, innan frá og utan, vísvitandi og óviljandi. Markmið stjórnunar upplýsingaöryggis er að tryggja áframhaldandi aðgang að upplýsingum nemendaskrár og lágmarka tjón, ef skaði verður, með því að koma í veg fyrir eða lágmarka áhrif af atvikum sem geta truflað upplýsingavinnslu úr nemendaskrá eða upplýsingaleka.

Nemendaskrá inniheldur m.a. 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 Blönduskóli þessa öryggisstefnu er varðar trúnað, réttleika og tiltækileika gagna.

Trúnaður. *Blönduskóli* tryggir að eingöngu aðilar, sem til þess hafa heimild, hafi aðgang að upplýsingum nemendaskrár og búnaði tengdum henni.

Réttleiki gagna. *Blönduskóli* tryggir að upplýsingar sem skráðar eru í nemendaskrá séu réttar og nákvæmar á hverjum tíma. Rangar, villandi, ófullkomnar eða úreltar upplýsingar séu leiðréttar, þeim eytt eða við þær aukið þegar slíkt uppgötvast og haldið uppi reglubundnu eftirliti í þeim tilgangi.

Tiltækileiki gagna. *Blönduskóli* tryggir að upplýsingar skráðar í nemendaskrá séu aðgengilegar þeim sem hafa heimild og þurfa að nota þær þegar þeirra er þörf. Skólinn tryggir einnig að kerfi og gögn nemendaskrár 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 meðferð 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, þ.m.t. nemendaskrár, 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.

Blönduós, 1. ágúst 2018

Skólastjóri *Blönduskóla* Formaður *fræðslunefndar*

Ítarleg stefna

Markmið og leiðir:
Það er markmið *skólans* að nota raunhæfar, viðeigandi, hagnýtar og árangursríkar öryggisráðstafanir til að vernda mikilvæg verkferli og verðmæti nemendaskrár[1]. Sérstaklega skal tryggja að:

- aðgengi að upplýsingaverðmætum sé bundið við þá sem til þess hafa heimild;
- upplýsingaverðmæti séu varðveitt á tryggilegan hátt;
- farið sé að lögum um grunnskóla og persónuvernd varðandi aðgang, vinnslu, flutning, varðveislu og dreifingu upplýsinga;
- haldin sé viðeigandi leynd og trúnaður um upplýsingaverðmæti;
- réttleiki upplýsingaverðmæta sé tryggður með því að verja þau 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 nemendaskrá;
- 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 nemendaskrá og upplýsingaverðmætum tengdum skránni. Í henni er skilgreint lágmarksöryggi.

Ábyrgð og skipulag:
1. Skólastjóri er endanlega ábyrgur fyrir öryggi upplýsingaverðmæta sem skólinn skráir í nemendaskrá.
2. Skólastjóri skipar tilsjónarmann persónuverndar sem sér um daglega tilsjón persónuverndar og upplýsingaöryggis tengt notkun á nemendaskrá.
3. Tilsjónarmaður persónuverndar skal sjá til þess að starfsfólk sem notar nemendaskrá eða gögn úr kerfinu hljóti viðeigandi fræðslu um persónuvernd og öryggismál. Verksvið tilsjónarmanns er að öðru leyti skilgreint í reglubók.
4. Tilsjónarmaður persónuverndar skal vera tengiliður við forsjármenn, Persónuvernd og persónuverndarfulltrúa, ef tilsjónarmaður er ekki jafnframt persónuverndarfulltrúi, vegna mála er varða friðhelgi og vernd persónugreinanlegra upplýsinga.
5. Skólastjóri er ábyrgur fyrir því að allir hlutaðeigandi starfsmenn skólans þekki og skilji öryggisstefnu þessa og hafi hana að leiðarljósi í starfi sínu. Skólastjóri getur falið tilteknum starfsmanni daglega framkvæmd þessa þáttar.
6. Það er á ábyrgð sérhvers starfsmanns að fylgja þessari öryggisstefnu og öryggisreglum sem koma fram í reglubók vegna nemendaskrá.

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 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 áhættumati og greiningu á öryggiskröfum laga og opinberra eftirlitsaðila.

[1] Grunnskólinn heldur skrá yfir alla nemendur skólans og heldur utan um upplýsingar sem hann safnar, skráir eða fær afhentar vegna skólavistar nemandans í nemendaskrá. Upplýsingarnar geta verið rafrænar eða á raunlægum miðlum, þ.m.t. pappír.

4. Velja skal viðeigandi tæknilegar og skipulagslegar öryggisráðstafanir til að vernda upplýsingaverðmæti. Öryggisráðstafanir skal endurskoða samhliða endurmati á öryggisstefnu og áhættumati.
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 nemendaskrár 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 tilsjónarmaður persónuverndar hafa eftirlit með þeim.
2. Um aðgang nemenda og forsjármanna að nemendaskrá gilda strangar öryggisreglur sem nánar eru tilgreindar í reglubók og tengdum verklagsreglum. Skal þeim greint frá þeim með skriflegum hætti áður en aðgangur er veittur.
3. Aðgangsheimildum nemendaskrár skal ætíð viðhaldið og breytingar á stöðu notenda skulu án tafar tilkynntar til rekstraraðila aðgangsstjórnunar.
4. Allur gagnaaðgangur í nemendaskrá skal skráður og skilja eftir úttektarslóð sem safnað er í rekstrardagbók.
5. Skólastjóri skal hafa eftirlit með aðgangi og notkun upplýsinga í nemendaskrá. 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 skólans til að tengjast rafrænni nemendaskrá 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. 77/2000 um persónuvernd og meðferð persónuupplýsinga, reglna nr. 299/2001 um öryggi persónuupplýsinga og reglugerðar Evrópuþingsins og ráðsins (ESB) 2016/679. Varðandi söfnun, vinnslu, flutning, vörslu og dreifingu persónuupplýsinga skal eftirfarandi að lágmarki virt:
    a. Að upplýsingarnar séu unnar með sanngjörnum, málefnalegum og lögmætum hætti og að öll meðferð þeirra sé í samræmi við vandaða vinnsluhætti persónuupplýsinga.
    b. Að upplýsingarnar séu fengnar í yfirlýstum, skýrum, málefnalegum tilgangi og ekki unnar frekar í öðrum og ósamrýmanlegum tilgangi.
    c. Að upplýsingarnar séu nægilegar, viðeigandi og ekki umfram það sem nauðsynlegt er miðað við tilgang vinnslunnar.
    d. Að upplýsingarnar séu áreiðanlegar og uppfærðar eftir þörfum, persónuupplýsingar sem eru óáreiðanlegar eða ófullkomnar, miðað við tilgang vinnslu þeirra, skal afmá eða leiðrétta.
    e. Að skólinn geti sýnt fram á hann hlíti lögum og reglum sem gilda um vinnsluna.
    f. Að til staðar séu viðeigandi tæknilegar og stjórnunarlegar aðgerðir til að verja réttindi hins skráða.
    g. Að hinum skráða sé gerð grein fyrir rétti sínu til að vita hvaða upplýsingar eru skráðar og fá rangar upplýsingar leiðréttar.

h. Að upplýsingum um hinn skráða sé þá aðeins deilt með þriðja aðila, að fyrir liggi samþykki hins skráða/forsjármanna eða að miðlun þeirra styðjist við heimild í lögum.
i. Að hinn skráði/forsjármenn 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 nemendaskrá skulu vera skráðar rétt og á nákvæman hátt miðað við upplýsingagjöf.
3. Rangar, villandi, ófullkomnar og úreltar upplýsingar skal leiðrétta, eyða eða við þær aukið þegar þær uppgötvast og halda skal uppi reglubundnu eftirlitsferli í þeim tilgangi.
4. 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.
5. Setja skal upp varnir gegn spilliforritum til að tryggja leynd, réttleika og aðgengileika gagna. Reglur um það skulu settar fram í reglubók.
6. Starfsmenn skulu undirrita yfirlýsingum um að halda trúnað um upplýsingar í nemendaskrá, 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 skólans.

Neyðarstjórnun og öryggisfrávik:

1. Tryggja skal samfelldan rekstur upplýsingakerfa nemendaskrár í samræmi við niðurstöðu áhættumats.
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 *skólanum* með skriflegum verklagsreglum um útfærslu öryggisstefnunnar.
2. Í reglubókinni skal að lágmarki vera:
   - upplýsingar um skólann og viðeigandi öryggisþarfir;
   - rammi öryggisstjórnunar, þ.e. hvernig öryggismálum er stjórnað; - verksvið tilsjónarmanns, trúnaðaryfirlýsing, fræðsla um kerfið og fl.
   - lýsing á upplýsingaöryggiskerfi;
   - tilvísunarskrá þar sem vísað er í ítarefni og nánari verkferli;
   - lýsing á þeim aðferðum sem notaðar eru við áhættumat;
   - 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. *Skólinn* skal uppfylla gildandi lög og reglugerðir sem lúta að vinnslu í nemendaskrá og annarra 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).