



Vinnureglur

fyrir notkun Copilot og annarra mállíkana há embætti landlæknis

Embætti landlæknis

Tilgangur

Að tryggja örugga, ábyrga og lögmæta notkun Copilot og annarra mállíkana. Hafa þarf í huga að mállíkon kunna að vista allt efni sem sett er inn í þau.

Þessar vinnureglur eru almenns eðlis og eiga við um Copilot sem og önnur mállíkon sem embættið veitir starfsmönnum aðgang að (t.d. ChatGPT og Claude).

1. Almenn öryggisviðmið

- Settu **aldrei** inn persónuupplýsingar.
- Notaðu eingöngu gervigreindartól sem embætti landlæknis hefur áskrift að í störfum þínum fyrir embættið.
- Settu **ekki** inn trúnaðarupplýsingar úr innri kerfum (t.d. málaskrá) eða skjölum.
- Ekki hlaða upp skjölum, myndum eða texta sem innihalda viðkvæm gögn og/eða gögn sem rekja má til einstaklings.
- Notaðu aðeins **almennt, nafnlaust og/eða ópersónugreinanlegt** efni.
- Ef vafi vaknar: **Settu það ekki inn.**
- Hafðu í huga að gervigreindin getur haft rangt fyrir sér.

2. Óheimil notkun Copilot

Copilot má ekki nota til að:

- Vinna með eða lýsa raunverulegum málum einstaklinga.
- Endurskapa, afrita eða lýsa efni úr sjúkraskrá eða öðrum viðkvæmum gögnum.
- Senda texta, myndir eða skjöl úr innri kerfum (t.d. skjáskot).
- Útskýra eða vinna með trúnaðarupplýsingar um öryggismál embættis landlæknis eða þau stafrænu kerfi sem notuð eru í skjalavörslu, þ.e. málaskrá.
- Vinna úr gögnum sem gætu talist persónuupplýsingar, þó að nöfn séu fjarlægð.

3. Leyfileg notkun Copilot og annarra mállíkana

Copilot má nota til:

- Almennrar útskýringar á lögum, verklagi eða faglegum hugtökum (án raunmála).
- Aðstoðar við textavinnu sem ekki er viðkvæm, t.d. sniðmát, verklagslýsingar og vinnuferla.
- Hugmynda- og skipulagsvinnu (t.d. til að gera verkefnalista, flæðirit og yfirlit).
- Tæknilegrar aðstoðar í Office-forritum eða almennri upplýsingatækni, s.s. við að setja upp glærukynningar og notkun excel.
- Að fræða um gagnavernd og persónuvernd.
- Heimildaleitar, t.d. um regluverk í öðrum löndum, klínískar leiðbeiningar um tiltekið efni, o.s.frv. Nauðsynlegt er að yfirfara þær heimildir sem mállíkanið vísar til.

4. Hvernig á að spyrja Copilot á öruggan hátt?

- Gefið mállíkaninu skýr og nákvæm fyrirmæli.
- Gefið mállíkaninu fyrirmæli um að geta ekki í eyður ef það finnur ekki upplýsingar og að gefa alltaf upp heimildir.
- Ef oft er verið að spyrja um svipaða hluti er gott að eiga góðan texta og spurningar.
- Gott er að nota alltaf nýtt spjall ef spyrja á eða afla upplýsinga um nýtt málefni, þar sem Copilot getur annars blandað saman ólíkum málefnum í svörum sínum.
- Prófaðu að spyrja Copilot um flókin málefni sem þú þekkir vel og rýndu þær niðurstöður. Oft koma fram villur, sem er góð áminning um að það sama á við um flest annað sem þú kannt að nýta Copilot við.

5. Ábyrgð notanda

- Notandi ber **ábyrgð á öryggi** þess efnis sem hann setur inn.
- Meta skal hvort efni sé viðkvæmt **áður** en byrjað er að skrifa eða líma texta inn í mállíkan.
- Mikilvægt er að yfirfara og sannreyna niðurstöður frá Copilot og öðrum mállíkönum áður en þær eru notaðar í vinnu.

6. Meðferð á afurð frá Copilot

- Afurðir Copilot eru **ekki sjálfkrafa nothæfar**. Gervigreind getur skilað röngum niðurstöðum og því nauðsynlegt að yfirfara og sannreyna afurð/skjal og aðlaga.

7. Endurskoðun og fræðsla

- Endurskoða skal þessar vinnureglur einu sinni á ári og uppfæra eftir þörfum.
- Starfsfólk skal fá reglubundna og markvissa fræðslu um örugga notkun gervigreindar og um persónuvernd.