Tietoturva- ja tietosuojapolitiikka

Tietoturva- ja tietosuojaohjeet, versio 4.3.2024

Käsitelty: YT-ryhmä 14.03.2024, Johtoryhmä, 03.04.2024

Hyväksytty: Hallitus 09.04.2024

Sisällys

Kuvat

1 Tietoturva- ja tietosuojapolitiikka

Tietoturvapolitiikka on Kpedun johdon kannanotto, joka määrittelee tietojen turvaamisen tavoitteet, vastuut, toteutuksen ja seurannan.

Tietosuojapolitiikan tarkoitus on määritellä ne pääperiaatteet, vastuut ja toimintatavat, joita Kpedussa noudatetaan henkilötietoja käsiteltäessä.

Tämä tietoturva- ja tietosuojapolitiikka on kaikkien työntekijöiden, jäsenten ja yhteistyökumppaneiden saatavilla, ja sen noudattamista edellytetään.

1.1 Tavoite

Ensisijainen tavoite on suojata henkilötietoja, tietopääomaa, resursseja ja infrastruktuuria luvattomalta käytöltä, vahingoittamiselta tai häviämiseltä. Tarkoituksena on varmistaa oppilaitoksen tietojärjestelmien, verkkojen, tietokoneiden, tiedon ja muiden tietoteknisten resurssien eheys (tieto pysyy muuttumattomana), luottamuksellisuus (kukaan sivullinen ei saa tietoa) ja käytettävyys (tieto on hyödynnettävissä).

Henkilötietojen käsittely tapahtuu aina lainmukaisen oikeusperusteen pohjalta ja määriteltyä tarkoitusta varten. Tietoja käsitellään lainmukaisesti, asianmukaisesti ja läpinäkyvästi, sekä ainoastaan niin kauan ja siinä määrin kuin on tarpeellista. Rekisteröityjä informoidaan asianmukaisesti ja oikea-aikaisesti henkilötietojen käsittelystä sekä rekisteröidyn oikeuksista. Henkilötietojen käsittelystä on laadittu tietosuojaselosteet. Rekisteröityjen oikeuksiin liittyvät pyynnöt käsitellään määritellyn prosessin mukaisesti. Henkilötietojen käsittely suunnitellaan etukäteen. Tietosuojavaatimusten noudattamisesta ja dokumentoinnista huolehditaan suunniteltaessa uusia palveluita, sovelluksia tai prosesseja, joihin liittyy henkilötietojen käsittelyä.

1.2 Vastuut ja valtuudet

Tietoturvallisuus ja tietosuoja ovat osa koulutusyhtymän kokonaisturvallisuutta. Tietoturvaan ja tietosuojaan nimetyt vastuut ja tehtävät ovat:

- **Jokaisen** tietoa, digitaalisia työvälineitä ja/tai tietoverkkoja käyttävän edellytetään toimivan vastuullisesti.
- **Yhtymähallitus** ohjeistaa salassapito- ja tietosuojavelvoitteiden noudattamisesta (hallintosääntö)

- **Talousjohtaja** vastaa yhteisten tietojärjestelmien ja tietohallinnon koordinoinnista. Talousjohtaja päättää yhteisiin tietojärjestelmiin, lisensseihin ja IT-laitteisiin liittyvistä sopimuksista (hallintosääntö).
- **Päälliköt ja esihenkilöt** vastaavat henkilöstörekisteriasioiden, arkistoasioiden sekä tietoturva- ja tietosuoja-asioiden asianmukaisesta hoidosta (hallintosääntö).
- Tietojärjestelmien ja niiden sisältämien **tietojen omistaja** vastaa tietojensa ja tietojärjestelmiensä huolellisesta käytöstä, sekä rekisteriselosteiden ylläpidosta.
- Tietosuojan asiantuntijana toimii **tietosuojavastaava** (tehtävän kuvaus on hallintosäännössä). Tekee mahdolliset tarvittavat viranomaisilmoitukset.
- Tietoturvan asiantuntijana toimii **tietoturvavastaava**. Tietoturvavastaava koordinoi tietoturvaan liittyviä asioita, seuraa tietoturvallisuuden tilaa ja tekee perusteltuja tietoturvan kehittämisesityksiä talousjohtajalle.
- **IT-palvelut ja tietohallinto** yhdessä tai erikseen viestittää henkilöstölle ja opiskelijoille ajankohtaisista tietoturvavaaroista ja/tai haavoittuvuuksista.
- Häiriö-, poikkeus- ja kriisitilanteissa on **IT-palvelujen tai tietohallinnon asiantuntijalla** valtuus tehdä väliaikaiset, akuutit ja välttämättömät ensitoimet vahinkojen minimoimiseksi tai estämiseksi.
- Häiriö-, poikkeus- ja kriisitilanteissa **valmiusryhmä** yhdessä IT-palvelujen ja tietohallinnon kanssa koordinoi toimenpiteitä vahinkojen minimoimiseksi ja tilanteen korjaamiseksi sekä tilanteesta palautumiseksi. Viestinnästä häiriö-, poikkeus- ja kriisitilanteissa vastaa kuntayhtymän johtaja (varahenkilö: rehtori) hallintosäännön mukaisesti. Päättää kuka tekee tarvittaessa rikosilmoituksen.
- **Käyttäjä** vastaa oman toimintansa tietoturvallisuudesta ja tietosuojasta. Käyttäjä on velvollinen noudattamaan tätä tietoturva- ja tietosuojapolitiikkaa ja ilmoittamaan IT-palveluille havaitsemistaan tietoturvapoikkeamista ja tietosuojaloukkauksista PRO24-lomakkeella. Henkilöstön ja opiskelijoiden on käsiteltävä tietoja huolellisesti ja vain niissä tarkoituksissa, joita varten ne on annettu/tehty. Luottamuksellisten tietojen käsittelyssä on noudatettava erityistä huolellisuutta, ja tietoja saa käyttää vain oikeutettuihin tarkoituksiin. Tietojen luvaton jakaminen tai siirtäminen ulkopuolisille on kiellettyä.

1.3 Toteutuskeinot

Tietoturvallisuuden ja tietosuojan ylläpito on jatkuva prosessi, joka tapahtuu hallinnollisten, fyysisten ja teknisten ratkaisujen avulla. Tarvittaessa tehdään kehittämissuunnitelmia. Käyttäjien toimintaa ohjataan käyttöohjeilla, toimintaohjeilla sekä erilaisilla koulutuksilla.

Hallinnon julkisuusperiaatteen mukaan viranomaisen asiakirjat ovat julkisia ja niiden salassapidosta säädetään laissa viranomaisten toiminnan julkisuudesta (621/1999). EU:n yleisen tietosuoja-asetuksen (2016/679) velvoitteilla toteutetaan yksityisyyden suojaa henkilötietoja käsiteltäessä.

Tietojen luokittelumallin tarkoitus on selkeyttää mihin tietoja voidaan julkaista ja tallentaa. Luokittelumalli on seuraava: julkinen; osittain salassa pidettävä; salassa pidettävä

1. Julkinen tieto

- Tiedon katseluun tai tallentamiseen ei ole rajoituksia.
- Julkaisuissa on huomioitava tekijänoikeudet.
- Esimerkkejä julkisista tiedoista ovat lehdistötiedotteet, kurssitiedot, tutkimusjulkaisut, julkiset asiakirjat ja julkiset www-sivustot.
- Aineistoa voidaan tulostaa ja tulosteet hävittää paperinkeräykseen.

2. Osittain salassa pidettävät

- jos asiakirjan luovuttaminen on lain mukaan viranomaisen harkinnassa tai asiakirjaan sisältyviä tietoja saa lain mukaan käyttää tai luovuttaa vain määrättyyn tarkoitukseen ja jos tiedon oikeudeton paljastuminen voi aiheuttaa haittaa yleiselle tai yksityiselle edulle tai heikentää viranomaisen toimintaedellytyksiä.
- Tietoa ei saa tallentaa kotitietokoneelle tai julkiseen käyttöön tarkoitettuun tietokoneeseen, julkisille internetsivuille tai sosiaaliseen mediaan.
- Aineistoa voi tulostaa omaan käyttöön ja se tulee hävittää tietoturvasäiliöön.
- Kaikki keskeneräiset asiakirjat, esim. keskeneräiset opintosuoritukset, hankkeet tai projektit.

3. Salassa pidettävä tieto

- Tietoa voivat katsella ja käsitellä vain erikseen valtuutetut henkilöt.
- Tieto voidaan tallentaa vain asianmukaisiin tietojärjestelmiin. Aineistoa voidaan tulostaa omaan käyttöön, mutta sen säilyttämisessä tulee huomioida tietoturvallisuus. Aineisto hävitetään tietosuojasäiliöön.
- Salassa pidettävää tietoa ovat esim. henkilötiedot, tiedot henkilön terveydentilasta, vammaisuudesta, terveydenhuollon tai sosiaalihuollon asiakkuudesta tai kuntoutuksesta (esim. hakemukset ja päätökset erityisjärjestelyistä opinnoissa), etnisestä alkuperästä, poliittisista mielipiteistä, uskonnosta tai vakaumuksesta, tiedot henkilön vuosituloista tai kokonaisvarallisuudesta taikka tuen tai etuuden perusteena olevista tuloista ja varallisuudesta taikka jotka muutoin kuvaavat hänen taloudellista asemaansa jne. Lisäksi mm. turvallisuusjärjestelyihin liittyvä tieto on salassa pidettävää.

Tietojärjestelmille on nimetty vastuuhenkilöt ja tietojärjestelmät on luokiteltu kriittisyyden perusteella. Tietojärjestelmien luokittelulla on merkitystä esim. mahdollisen kyberhyökkäyksestä toipumisen yhteydessä. Tietojärjestelmien luokittelu:

1. järjestelmät, jotka vaikuttavat koko Kpedun toimintaan,
2. muut henkilötietoja sisältävät järjestelmät,
3. eläinten turvallisuuteen vaikuttavat järjestelmät (esim. navetta) ja
4. muut järjestelmät.

1.4 Tietoturvallisuuden ja tietosuojan seuranta ja ongelmatilanteiden käsittely

Kuntayhtymän johtajalla, talousjohtajalla, tietohallintopäälliköllä, tietosuojavastaavalla, tietoturvavastaavalla ja IT-palveluvastaavalla on valtuutus ja velvollisuus tehdä koulutusyhtymän tietojärjestelmien tietoturvallisuuden kartoituksia ja ryhtyä toimenpiteisiin havaittujen puutteiden korjaamiseksi.

Käyttäjien tulee ilmoittaa havaitsemistaan tietoturvallisuuden puutteista, tietoturvallisuuteen liittyvistä väärinkäytöksistä tai epäilemistään tietoturvarikkomuksista tai tietosuojarikkomuksista PRO24-lomakkeella (turvallisuustyöpöydän Tietoturva ja tietosuoja -sivulla).

1.5 Vastuullisuus

Vastuullisuus tarkoittaa pyrkimystä käyttää digitaalisia laitteita ja järjestelmiä tavalla, joka ottaa huomioon ympäristön, yhteiskunnan ja eettiset näkökulmat. Tärkeitä periaatteita ja käytäntöjä vastuullisuuden edistämiseksi ovat:

1. Ympäristövastuu:

- Valitsemme mahdollisimman ympäristöystävälliset laitteet ja komponentit.
- Vähennämme energiankulutusta optimoimalla laitteiden käyttöä ja käyttämällä energiatehokkaita asetuksia.
- Kierrätämme vanhat laitteet ja elektroniikkaromun asianmukaisesti.
- Kierrätämme mahdolliset tulosteet ja asiakirjat keräyspaperiksi tai tietosuojasäilössä tuhottaviksi.

2. Eettinen käyttäytyminen:

- Kunnioitamme käyttäjien yksityisyyttä ja tietosuojaa. annamme käyttäjille selkeää tietoa siitä, miten heidän tietojaan kerätään, käytetään ja jaetaan.
- Käytämme selkeää ja ymmärrettävää kieltä ohjeissa ja tiedotteissa (selkokieli).
- Kunnioitamme käyttäjän antamaa suostumusta tietojen keräämiseen ja käyttämiseen. Määrittelemme selkeästi, miten suostumus pyydetään ja miten käyttäjä voi sen peruuttaa.

- Määrittelemme tarkasti, mihin tarkoitukseen kerättyjä henkilötietoja käytetään.
- Vältämme syrjintää, rasismia ja muuta epäasiallista käyttäytymistä verkossa.
- Varmistamme, että ohjelmistoilla ja palveluilla ei edistetä haitallisia käytäntöjä, kuten esim. vihapuhetta tai väärän tiedon leviämistä.

3. Sosiaalinen vastuu:

- Toteutamme tasa-arvoa ja monimuotoisuutta teknologia-alalla.
- Pyrimme vähentämään digitaalista kuilua tarjoamalla saavutettavia digipalveluita henkilöstöllemme, opiskelijoillemme ja sidosryhmillemme (digipalvelujen saavutettavuus).
- Tarjoamme koulutusta ja tietoa digipalvelujen turvallisesta käyttämisestä ja digitaaliseen ympäristöön liittyvistä vaaroista sekä niiltä suojautumisesta.

4. Turvallisuus:

- Huolehdimme tietojen turvallisuudesta ja suojaamisesta asianmukaisilla turvallisuuskäytännöillä ja teknisillä ratkaisuilla.
- Käytämme järjestelmiä ja sovelluksia, jotka suojaavat käyttäjiä haitallisilta hyökkäyksiltä, kuten hakkereilta ja tietomurroilta.
- Tarjoamme käyttäjille tietoa, ohjeita ja työkaluja omien tietoturvakäytäntöjensä parantamiseksi.

5. Talousvastuu:

- Käytämme resursseja tehokkaasti ja vältämme turhia kustannuksia.
- Arvioimme teknologiaratkaisujen taloudellisia ja liiketoiminnallisia vaikutuksia pitkällä aikavälillä.
- Otamme huomioon sekä sisäisten, että ulkoisten sidosryhmiemme tarpeet ja odotukset.

Vastuullisuus on jatkuva prosessi, joka vaatii sitoutumista ja jatkuvaa kehitystä sekä kehittämistä.

1.6 Tietoturva- ja tietosuojapolitiikan päivitys

Tietoturvapolitiikkaa katselmoidaan vuosittain ja päivitetään säännöllisesti vastaamaan muuttuvia tietoturvatarpeita, lainsäädäntöä ja teknologisia kehityksiä. Päivitykset ja muutokset tietoturvapolitiikkaan viestitään asianosaisille, ja tarvittaessa järjestetään koulutusta ja tiedotustilaisuuksia.

2 Tietoturva- ja tietosuojaohjeita

Jokaisen käyttäjän tulee huolehtia tietoturvallisuuteen liittyvistä asioista. Kaikilla käyttäjillä on oma vastuunsa tietojärjestelmän kokonaisturvallisuudesta.

Toista käyttäjää koskevien tai hänelle kuuluvien tietojen etsiminen ja lukeminen on sallittu vain hänen luvallaan tai jos työtehtävät sitä vaativat. Mikäli käyttäjä saa vahingossa haltuunsa muille osoitettuja tai kuuluvia tietoja, on niiden hyväksikäyttö, talteenotto ja levittäminen kiellettyä. Tapahtumasta on ilmoitettava järjestelmän ylläpidolle ja asianomaiselle käyttäjälle.

IT-palvelujen henkilöstö huolehtii verkkoon tallennettujen tietojen varmuuskopioinnin. Vaikka tietokonejärjestelmien ja tietoliikenneverkon käytettävyys pyritään pitämään mahdollisimman korkeana, ei käyttöhäiriöiltä kuitenkaan voida kokonaan välttyä. Vastuu tietoaineistojen säilymisestä on viime kädessä aineiston omistajalla itsellään.

Keski-Pohjanmaan koulutusyhtymä ei vastaa käyttäjälle aiheutuneesta vahingosta tai menetyksestä, joka johtuu Keski-Pohjanmaan koulutusyhtymän tietojärjestelmien käytöstä.

2.1 Pääsynhallinta, käyttöoikeudet ja tunnistautuminen

Pääsynhallinta tarkoittaa järjestelmää tai prosessia, jolla säännellään käyttäjien tai käyttäjäryhmien oikeuksia ja mahdollisuuksia käyttää tiettyjä järjestelmiä, resursseja tai tietoja. Se sisältää käyttäjätunnistusta, käyttöoikeuksien määrittelyä ja valvontaa sekä erilaisten tietojen ja toimintojen rajoittamista. Pääsynhallinta on tärkeä osa tietoturvaa ja auttaa varmistamaan, että vain oikeutetut käyttäjät pääsevät käsiksi tarvittaviin tietoihin ja toimintoihin.

Pääsynhallinnan periaatteet Kpedussa:

1. Tarpeenmukaisuus: Käyttäjille myönnetään vain ne pääsyoikeudet, jotka ovat tarpeen heidän työtehtäviensä suorittamiseen. Liiallisten oikeuksien välttäminen minimoi turvallisuusriskejä.
2. Vähimmän oikeuden periaate: Käyttäjille myönnetään vain tarvittavat oikeudet, jotta he voivat suorittaa työtehtävänsä. Näin pyritään minimoimaan mahdollisten vahinkojen laajuus, jos käyttäjätunnuksiin kohdistuu hyökkäys tai ne joutuvat vääriin käsiin.

Esihenkilö tilaa työntekijälle tarvittavat pääsyoikeudet Kpedun järjestelmiin lomakkeella, joka löytyy Wihtori -> Henkilöstöpalvelut -> Palvelussuhdeasiat -> Palvelussuhteen alkaessa -> Tilauslomake tunnusten, oikeuksien ja työvälineiden hankintaan, lukitsemiseen ja päättämiseen. Samalla

lomakkeella esihenkilö ilmoittaa myös työntekijän palvelussuhteen päättymisestä. Pääsyoikeuksien muutokset tehdään aina esihenkilön kautta tarvearvioinnin perusteella.

Pääkäyttäjät katselmoivat säännöllisesti (vähintään puolivuosittain) oman järjestelmänsä käyttöoikeuksia ja tekevät tarvittavat muutokset.

Kpedussa käytetään monivaiheista tunnistautumista (MFA = Multi-Factor Authentication). Monivaiheisella tunnistautumisella tarkoitetaan sitä, että henkilöllisyys varmistetaan kahta tai useampaa eri tunnistautumistapaa käyttämällä. Lähes kaikki käyttäjätilien kaappausyritykset voidaan estää monivaiheista tunnistautumista käyttämällä. Tästä huolimatta käyttäjätunnuksen ja salasanan kanssa tulee olla huolellinen.

Käyttäjätunnus ja siihen liittyvä salasana ovat henkilökohtaisia eikä niitä saa luovuttaa muiden käyttöön. Salasana, joka on saattanut tulla toisen henkilön tietoon, on pikaisesti muutettava. Kaikki Kpedun käyttäjätunnukset vääriin käsiin joutuessaan ovat merkittävä tietoturvariski, jonka realisoituminen pahimmillaan voi aiheuttaa koko Kpedun toiminnan keskeytymisen.

Kukin käyttäjä vastaa omalla tunnuksellaan tapahtuvasta käytöstä. Tämän vuoksi myös erilaiset ”yleistunnukset” ovat kiellettyjä/mahdottomia käyttää. Järjestelmiä on käytettävä yleisesti ottaen huolellisesti ja hyvän tavan mukaisesti. Käyttäjä vastaa itse omien tiedostojensa ja tallennusvälineidensä suojauksesta.

2.2 Opetustiloissa työskentely ja/tai opetuskäyttöön tarkoitettujen digitaalisten laitteiden käyttö

Kpedun tiloissa olevat digitaaliset laitteet ovat pääsääntöisesti vain opiskelijoiden tai henkilökunnan käytettävissä. Opetukseen tarkoitettujen laitteiden käytön tärkeysjärjestys on:

1. opetushenkilöstön johdolla tapahtuva opetus/ohjaus
2. muut mahdolliset työt (esim. harjoitustehtävien tekeminen).

2.3 Mobiililaitteet

Kaikki Kpedun työkäyttöön annetut mobiililaitteet rekisteröidään keskitettyyn hallintapalveluun. Mobiililaitteisiin asennetaan tarvittava tietoturvaohjelmisto automaattisesti. Työkäyttöön annettu mobiililaite on tarkoitettu vain työkäyttöön.

Käyttäjän tulee pitää oma mobiililaitteensa ajan tasalla ja asentaa järjestelmän päivitykset niiden ilmestyttyä. Myös sovellusten käyttöoikeudet kannattaa tarkistaa ja myöntää oikeuksia vain niille sovelluksille, joissa niitä tarvitaan (esim. mikrofonin ja kameran käyttöoikeus).

2.4 Tulostaminen ja tallentaminen

Opiskelijoilla ja henkilöstöllä on käytettävissään pilvitallennustilaa M365-palvelussa ja mahdollisesti verkkolevyjä. Tallennuksessa on huomioitava kohtuullisuus: suuret kuva- ja videotiedostot vievät paljon tallennustilaa ja aiheuttavat lisäkustannuksia tiedon varmistamisessa. Kpedun tallennustilaan saa tallentaa vain työhön tai opiskeluun liittyviä tiedostoja. Aineiston omistaja huolehtii vanhan tai vanhentuneen tiedon poistamisesta tallennustilasta.

Tulostamista vältetään ja tieto pyritään mahdollisimman pitkään käsittelemään digitaalisessa muodossa vastuullisuuden ja kestävän kehityksen mukaisesti. Tulostuksissa on noudatettava kohtuullisuutta ja toimittava Kopioston ohjeiden mukaisesti (tekijänoikeudet).

2.5 Ohjelmistojen luvaton käyttö ja kopiointi

Sovellusohjelman asentamiseen Kpedun tietokoneille tarvitaan aina IT-palvelujen lupa. Kpedun tietoverkossa ja tietokoneilla käytetään vain lisensoituja ohjelmia.

Laittomien ohjelmakopioiden (ns. piraattikopioiden) kopioiminen muualta, tallettaminen Kpedun järjestelmiin, jakelu tai suorittaminen Kpedun laitteissa on kielletty. Henkilöstön käytettävissä olevat sovellukset jaetaan yritysportaalin kautta.

Kpedun laitteille voidaan sallia erillisellä luvalla esim. opetukseen tai harjoitustyöhön liittyvien ohjelmien asentaminen. Tällöin ohjelma asennetaan tuotantokäytöstä eristettyyn tietokoneeseen (ns. labraverkko) tai eristetylle virtuaalipalvelimelle tai erikseen määrätylle tietokoneelle, joka ei ole yhteydessä Kpedun tietoverkkoon.

2.6 Sähköpostin käyttö

Monet virukset, haittaohjelmat ja tietojenkalasteluyritykset tulevat sähköpostin mukana, joko liitetiedostona tai linkkinä. Jokaisen tulee olla varovainen avatessasi linkkiä tai liitetiedostoa. Kaikkiin kirjautumispyyntöihin tulee suhtautua varauksella. Vaikka sähköposti näyttäisi tulevat tutulta lähettäjältä, kannattaa aina varmistaa lähettäjältä, onko liite tai linkki varmasti hänen lähettämänsä.

Kpedun sähköposti (kpedu.fi/student.kpedu.fi) on tarkoitettu ainoastaan työ - ja opiskeluasioiden hoitamiseen. Suurien sähköpostilistojen käyttöä on vältettävä. Massajakeluna tulleeseen sähköpostiin

vastaamisen kanssa tulee olla tarkkana, ettei vastaus välity koko henkilökunnalle. Kaikenlainen häirintä ja mainostaminen sähköpostilla on kielletty. Turha sähköpostitus kuormittaa henkilöstöä ja voi johtaa tarpeellisen tiedon hukkumiseen.

Koko Kpedulle tarkoitettu viestintä voi olla tarkoituksenmukaista tehdä esim. viikkotiedotteen välityksellä, ellei tiedon saamisella ole kiire. Opiskelijoita voidaan tiedottaa esim. wilmaviestien kautta.

2.7 Etätyön tietoturvallisuus

Etätyö on tullut jäädäkseen ja sitä tehdään paljon, mikäli työtehtävät sen sallivat. Etätyössä täytyy myös muistaa tietoturvallisuus:

- Etätyössä käytetään aina suojattua Wi-Fi-verkkoa tai jaetaan nettiyhteys omalta matkapuhelimelta (yhteydet --> mobiilitukiasema ja yhteyden jako).
- Työntekoon käytetään aina työpaikan tietokonetta ja/tai mobiililaitetta.
- Työsähköpostia lähetettäessä, käytetään aina työpaikan sähköpostitiliä (@kpedu.fi).
- Työasiat eivät kuulu edes perheelle; työaikana ja esim. Teams-kokouksissa on etsittävä rauhallinen paikka, missä voi puhua ja työskennellä rauhassa.
- Työpaikan papereita ei kuljeteta kotiin (tai muuhun etätyöpaikkaan), jollei se ole aivan välttämätöntä.
- Käytetään VPN-yhteyttä tarvittaessa.

2.8 Julkiset ja avoimet wifi-verkot

Avoin Wi-Fi on langaton lähiverkko, jossa ei vaadita salasanaa. Wi-Fi-verkko on käytännössä avoin myös silloin, kun salasana on kaikkien näkyvillä tai kuka vain voi sitä pyytää. Muut saman avoimen verkon käyttäjät voivat saada selville esimerkiksi salasanat tai käyttäjätunnukset. Verkkorikolliset käyttävät tähän ohjelmaa, joka nappaa dataliikenteen ja muuttaa sen tekstiksi näytölleen. Urkkijalle avoin verkko on kuin noutopöytä. Turvallisempi vaihtoehto on jakaa nettiyhteys omalta matkapuhelimelta.

Avoimessa WiFi-verkossa ei koskaan valita vaihtoehtoa ”Liitä automaattisesti”, ”Automaattinen yhdistäminen” tms. Yhteys katkaistaan, kun sitä ei enää tarvita. Avoimessa verkossa kannattaa välttää mm. pankkiasiointia, sähköpostiin kirjautumista, verkko-ostoksia ja muita salassa pidettäviä asioita.

2.9 Sosiaalinen media (esim. WhatsApp, Facebook, x)

Sosiaalista mediaa voidaan käyttää viestinnässä ja opetuksen tukena, mutta sen tietoturvaan ja tietosuojaan liittyen tulee huomioida nämä seikat:

- sosiaalisen median ohjelmistot/sovellukset eivät ole Kpedun hallinnassa.
- sosiaalisen median palveluihin ei tule tallentaa opiskelijoiden tietoja ilman suostumusta (esim. WhatsApp – puhelinnumero). Yli 16-vuotias voi antaa itse suostumuksen.
- Sosiaalisen median käytön tulee olla aidosti vapaaehtoista. Yhdenvertaisuuden nimissä kaiken sosiaalisessa mediassa jaetun tiedon tulee olla saatavissa myös muulla tavoin.
- Koska näillä sovelluksilla on ulkopuolinen rekisterinpitäjä, eikä Kpedu pysty kontrolloimaan tietojen käsittelyä tai mahdollista siirtoa EU:n ulkopuolelle, emme julkaise mitään tietosuojan alaista tai salassa pidettävää materiaalia niissä. Muista, että palvelun ylläpitäjät pääsevät teknisesti käsiksi kaikkeen palveluun talletettuun ja myös vain keskustelun osapuolten väliseksi rajoitettuun materiaaliin.
- Käytä erilaista salasanaa eri palveluissa. Käytä vain hyvänlaatuisia salasanoja. Älä käytä samoja käyttäjätunnuksia ja salasanoja työ- ja vapaa-ajan palveluissa.

Alla olevassa kuvassa on ohje opiskelijan henkilötietojen käyttämiseen eri verkkopalveluissa (kuva 1).

Opiskelijoiden henkilötiedot verkkopalveluissa

	Kpedun hallinnoimat palvelut (Wilma)	Kpedun hallinnoimat viestintä- ja oppimisalustat (esim. O365, Teams, Itslearning)	Ulkopuolinen sovellus, jossa tiedot eivät näy julkisesti (esim. Whatsapp, Quizlet)	Ulkopuolinen sovellus tai verkkopalvelu, jossa tiedot näkyvät julkisesti (esim. Padlet)
Käyttäjätunnukset ja niiden hallinnointi	Kpedu-IT:n luomat tunnukset	Kpedu-IT:n luomat tunnukset	Opettajan luomat tunnukset	Opettajan luomat anonyymit tunnukset tai ei tunnuksia
Saako opiskelija rekisteröityä palveluun itse koulussa?	Ok	Ok	Ok (yli 13-vuotiaat)	Ok (yli 13-vuotiaat)
Käyttö opetuksen aktivointiin, materiaalien jakoon ym.	Ok	Ok	Ok	Ok
Opiskelijoiden tekemät tehtävien palautukset ja esim. kuvat	Ok	Ok	Ok	Ei ilman suostumusta
Tavanomaisten henkilötietojen tallennus	Ok	Ok	Ei ilman suostumusta	Ei
Koetulokset ja arvosanat	Ok	Ok	Ei ilman suostumusta	Ei
Sanalliset arvioinnit, soveltuvuustestit ym.	Ok	Ei	Ei	Ei
Muut salassa pidettävät tiedot (esim. erityinen tuki, terveys)	Ok	Ei	Ei	Ei

Kuva 1 Opiskelijoiden henkilötietojen tallentaminen eri verkkopalveluissa.

2.10 Ulkoiset tallennusvälineet

Ulkoisten tallennusvälineiden käyttöä tulee välttää. Ne eivät ole tietoturvallinen tapa siirtää tietoa paikasta toiseen.

Ulkoisille tallennusvälineille (esim. USB-muistitikut) ei koskaan saa tallentaa sellaista tietoa, joka ei saisi päätyä ulkopuolisen käsiin (luottamukselliset tai salassa pidettävät tiedot). On oletettavaa, että muistitikku tai muu ulkoinen tallennusväline jossain vaiheessa katoaa, rikkoutuu tai unohtuu jonnekin. Suositeltavaa on tallentaa tieto esim. M365-palveluun, jolloin se on käytettävissä kaikkialla, missä on

verkkoyhteys. Pilvipalveluidenkin käytössä tulee muistaa, että työkäyttöön (ja vain työkäyttöön) käytämme työpaikan tarjoamaa pilvipalvelua (M365).

Mikäli välttämättä tarvitset muistitikkua tai muuta siirrettävää tietovälinettä, on se syytä salata (kryptata, salakirjoittaa), jolloin sen lukemiseen tarvitaan salasana. Tämä ei kuitenkaan ole varma keino tiedon suojaamiseksi.

Mikäli muistitikku (tai muu ulkoinen tallennusväline) katoaa ja se palautetaan myöhemmin, tulee siihen suhtautua varauksella – siihen on voitu ladata haittaohjelma.

2.11 Hybridivaikuttaminen

Hybridiuhissa on kyse pahantahtoisesta ulkoisesta vaikuttamisesta, jolla valtiollinen tai muu toimija pyrkii eri keinoja yhdistelemällä systemaattisesti vaikuttamaan kohteena olevaan maahan tai toimijaan. Hybridivaikuttamisen tavoitteena on hyödyntää kohteeksi valitun haavoittuvuuksia ja pyrkiä tekemään se mahdollisimman peitellysti.

Keinovalikoimaan voi kuulua esimerkiksi poliittista, taloudellista tai informaatio- ja kybervaikuttamista.

Hybridivaikuttamiselta voidaan suojautua suhtautumalla kriittisesti kaikkeen digitaaliseen tietoon (medialukutaito).

2.12 Tekoäly

Tekoälyn käyttäminen yleistyy koko ajan. Tekoäly on hyödyllinen työkalu, mutta siinä on myös omat riskinsä. Tekoälyn odottamattomia toimintoja voivat olla esim.:

1. Väärät päätökset ja virheelliset tulokset:
2. Tietoturvaloukkaukset ja hyökkäykset:

- Tekoälyjärjestelmät voivat olla alttiita tietoturvaloukkauksille ja hyökkäyksille, kuten hakkereiden manipuloinnille tai väärennetyille syötteille.
- Tekoälyä voidaan käyttää kyberhyökkäyksissä. Myös haittaohjelmat voivat käyttää tekoälytekniikoita, löytääkseen haavoittuvuuksia ja toteuttaakseen kohdennettuja hyökkäyksiä.
- Esimerkiksi pahantahtoiset toimijat voivat manipuloida kuvia tai ääntä.

3. Syrjivä toiminta:

- Tekoälyjärjestelmät voivat tuottaa syrjiviä tai epäreiluja tuloksia, jos niitä koulutetaan puutteellisella tai vinoutuneella datalla.
- Esimerkiksi rekrytointiprosesseissa tekoäly voi suosia tiettyjä sukupuolia, etnisiä ryhmiä tai muita demografisia tekijöitä koulutusdatan perusteella.

4. Inhimillisten ennakkoluulojen vahvistaminen:

- Tekoälyä voidaan käyttää manipuloimaan ihmisten käyttäytymistä verkossa esimerkiksi sosiaalisen median alustoilla. Tämä voi vaarantaa tietoturvaa ja altistaa käyttäjät haitalliselle sisällölle tai huijauksille.

5. Yllättävät tilanteet ja kontekstit:

- Tekoälyjärjestelmät voivat toimia odottamattomalla tavalla kohtaamalla uusia tai monimutkaisia tilanteita, joita ne eivät ole kohdanneet aiemmin.

6. Yksityisyyden riskit

- Tekoälyä voidaan käyttää keräämään ja analysoimaan valtavia määriä tietoa, mikä voi aiheuttaa yksityisyyden riskejä, jos tietoja ei käsitellä asianmukaisesti. Esimerkiksi henkilökohtaisten tietojen kerääminen ja analysointi tekoälyn avulla voi johtaa tietovuotoihin tai väärinkäyttöön.
- Tekoälyä voidaan käyttää profilointiin ja personointiin mainostarkoituksissa, mikä saattaa vaarantaa yksityisyyden, jos henkilökohtaisia tietoja käytetään ilman asianmukaista suostumusta.
- Tekoälyjärjestelmät voivat käsitellä ja muokata tietoja monimutkaisilla tavoilla, mikä voi tehdä tietojen alkuperän ja käsittelyn jäljittämisen vaikeaksi. Tämä heikentää yksilöiden mahdollisuuksia valvoa ja hallita omia tietojaan.
- Tekoälyä voidaan käyttää luomaan valheellisia tai manipuloituja tietoja, kuten kuvia, deepfake-videoita ja -äänitteitä. Tämä vaarantaa yksilöiden tietosuojan ja aiheuttaa vahinkoa heidän maineelleen ja turvallisuudelleen.

Nämä skenaariot korostavat tarvetta huolelliselle suunnittelulle, testaukselle ja seurannalle tekoälyn käytössä, jotta varmistutaan sen luotettavuudesta, turvallisuudesta ja vastuullisuudesta.

Jos pyydät tekoälyä analysoimaan tietoja, älä koskaan syötä sinne luottamuksellista tai salassa pidettävää dataa. Tekoälyalgoritmit, jotka käsittelevät arkaluontoisia tietoja, voivat olla haavoittuvia.

2.12.1 Tekoälyn käytön eettiset ohjeet

Tekoälyä käytettäessä noudatamme näitä eettisiä ohjeita ja opetamme nämä myös opiskelijoillemme. Autamme opiskelijoita kehittämään kykyä arvioida tekoälyn käyttöön liittyviä eettisiä kysymyksiä ja tekemään vastuullisia päätöksiä. Kannustamme heitä pohtimaan erilaisia vaihtoehtoja ja niiden seurauksia ennen päätöksentekoa. Vastuullisuus tekoälyn käytössä tarkoittaa huolellista ja harkittua lähestymistapaa tekoälyn käyttöön ja vaikutusten arviointiin.

- **Yksityisyys ja tietosuoja:** Kunnioita yksityisyyttä ja henkilötietojen suojaa tekoälyn käytössä. Huolehdi, että tietojen keruu, käsittely ja säilytys tapahtuu asianmukaisesti ja että käyttäjillä on mahdollisuus hallita omia tietojaan.

- **Rehellisyys ja luotettavuus:** Vältä harhaanjohtavaa tai manipuloivaa käyttöä tekoälyn avulla. Tavoittele totuudenmukaisia ja luotettavia tuloksia, ja varoita käyttäjiä mahdollisista rajoituksista tai virheistä tekoälyn toiminnassa.
- **Ihmiskeskeisyys ja hyvinvointi:** Varmista, että tekoälyn käyttö palvelee ihmisten tarpeita ja edistää heidän hyvinvointiaan. Vältä tekoälyn käyttöä, joka voi aiheuttaa haittaa tai vaarantaa ihmisten terveyttä, turvallisuutta tai autonomiaa.

2.13 Huolellisuusvelvoite

Tieturva- ja tietosuojaohjeiden noudattamisella, huolellisuudella ja varovaisuudella voidaan välttää monia kyberuhkia. Tietoturvallisuuden ja tietosuojan heikoin lenkki on aina ihminen.

Käyttöön annetun digitaalisen laitteet käsittelyssä tulee toimia huolellisesti. Matkustettaessa tulee olla erityisen varovainen, etteivät laitteet joudu vääriin käsiin. Mahdollisesta varkaudesta on ilmoitettava välittömästi IT-palveluille PRO24-lomakkeella, puhelimitse 044 725 0000 tai sähköpostilla helpdesk@kpedu.fi.

Huolellisuusvelvoite velvoittaa noudattamaan sovellettavia tietosuojalakeja ja -määräyksiä, kuten yleistä tietosuoja-asetusta (GDPR = General Data Protection Regulation) Euroopan unionissa. Tämä sisältää esimerkiksi velvollisuuden noudattaa tietosuojaperiaatteita, kuten oikeudenmukaisuutta, läpinäkyvyyttä ja tietojen oikeellisuutta.

Huolellisuusvelvoite kannustaa keräämään ja käsittelemään vain välttämättömät henkilötiedot tavoitteen saavuttamiseksi. Tämä auttaa vähentämään turhaa tietojenkäsittelyä ja minimoi riskin henkilötietojen väärinkäytöstä tai tietomurroista.