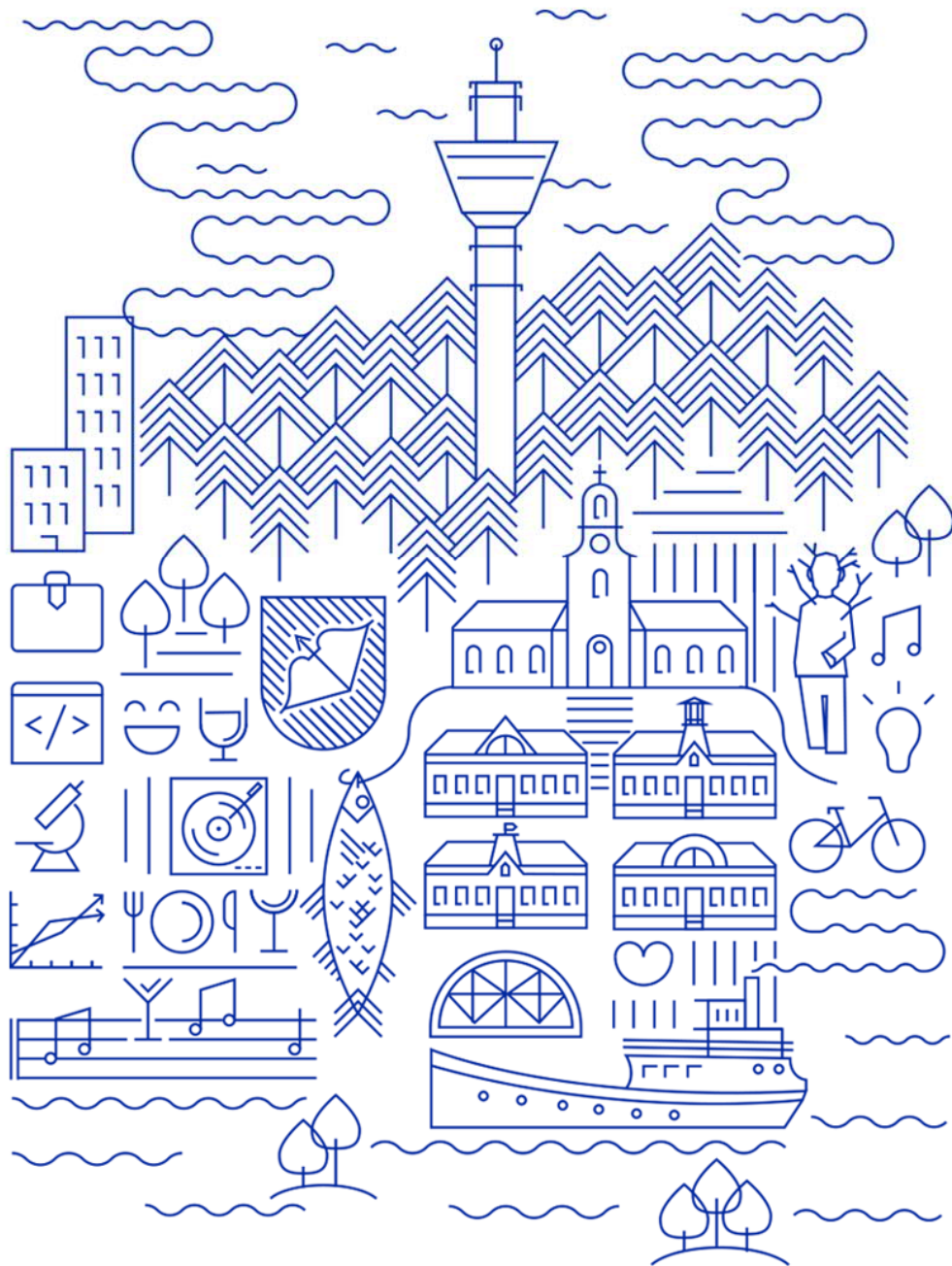


KUOPIO



Sähköisten viestintäpalveluiden käyttösäännöt Kuopion kaupunki

8.3.2021

Hyväksytty KH 31.5.2021 § 206

Sisällys

1 Työnantajan sähköisten viestintäpalveluiden käyttö	3
1.1 Johdanto.....	3
1.2 Työkäyttö ja yksityiskäyttö	3
1.3 Kielletyt toiminnot verkossa	4
2 Sähköposti.....	4
2.1 Määritelmät.....	4
2.2 Sähköpostiosoitteen muodostuminen ja julkaiseminen.....	5
2.3 Sähköpostiin liittyvät rajoitukset ja kiellot.....	5
2.4 Asiakkaalta tuleva sähköposti.....	7
2.5 Sähköpostien rajoittaminen ja suodattaminen	7
2.6 Perille menemättömät sähköpostiviestit	7
2.7 Väärään osoitteeseen saapuneet sähköpostiviestit	8
2.8 Palvelussuhteen väliaikainen katkeaminen ja päättyminen	8
2.9 Sähköpostin yksityinen käyttö	9
2.10 Luottamuksellinen sähköposti	9
3 Kaupungin Teamsin ja muiden videoneuvottelusovellusten kokouskäyttö.....	10
4 Pikaviestinten käyttö.....	10
4.1 Tekstiviestit	10
4.2 Sosiaalisen median viestintävälineet.....	11
4.3 Pikaviestimet.....	11
5 Sähköisen kalenterin käyttö.....	12
6 Tilanvarauskäytännöt	13
7 Pilvestä käytettävät palvelut	13
7.1 Maksulliset palvelut.....	13
7.2 Ilmaispalvelut.....	13
7.3 Yhteys tietohallintoon	14
8 Käytön valvonta sekä lokitietojen kerääminen ja säilyttäminen.....	14
9 Näiden sääntöjen valvonta.....	15
9.1 Yleiset periaatteet.....	15
9.2 Kuopion kaupungin tietoturva- ja tietosuojalinjaukset ja ohjeet	15

10 Keskeisiä lakeja	16
11 Sanasto	16

1 Työnantajan sähköisten viestintäpalveluiden käyttö

1.1 Johdanto

Kuopion kaupunki ohjeistaa tässä dokumentissa, mihin tarkoitukseen ja miten sähköisiä viestintäpalveluja ja tietoverkkoa käytetään. Näiden sääntöjen tarkoituksena on ohjeistaa käyttäjiä, varmistaa viestinnän osapuolten oikeusturva sekä parantaa verkon ja järjestelmien käytön tietoturvaa ja tietosuojaa.

Nämä säännöt koskevat kaikkia Kuopion kaupungin omistamien sähköisten viestintäpalveluiden käyttäjiä.

Ohjeessa olevat käsitteet on määritelty TEPA-termipankissa:

<http://www.tsk.fi/tsk/termitalkoot/>

1.2 Työkäyttö ja yksityiskäyttö

Tietotekniikkalaitteet ohjelmistoinen ja yhteyksineen on tarkoitettu työtehtävien hoitamiseen. Laittevalinnat on suunniteltu työkäytön mukaan. Työnantaja voi perustelluista syistä antaa työtehtävien hoitamista varten tietokoneen ohjelmistoinen ja/tai yhteyksineen henkilölle kotiin. Nämä säännöt koskevat näitäkin laitteita.

Työnantajan laitteita ja verkkoyhteyksiä ei saa käyttää yksityiseen yritys- tai yhdistystoimintaan eikä vastaaviin työtehtäviin liittymättömiin tehtäviin. Kielto ei koske ammattiyhdistystoimintaan liittyvää viestintää.

Pienimuotoinen yksityiskäyttö, kuten henkilökohtaisten laskujen maksaminen, on sallittua, ellei se haittaa työtehtävien hoitamista. Työnantaja ei ratko yksityiskäyttöön liittyviä ongelmia eikä vastaa henkilölle mahdollisesti koituneista vahingoista.

Jokainen käyttäjä on vastuussa siitä, että hänen tiedostonsa, sähköpostiviestinsä sekä Internet-käyttönsä on lakien, ohjeiden ja hyvän tavan mukaista. Työntekijän tulee muistaa viesteissään lojaliteettivelvollisuus työnantajaa kohtaan. Käyttäytymisen tulee olla asiallista riippumatta käytettävästä viestintävälineestä.

Sähköisten viestimien käyttäjien tulee miettiä, mitä riskejä omaan sähköiseen viestintään liittyy sekä pyrkiä huomioimaan ja minimoimaan kyseiset riskit. Internetistä löytyvään informaatioon ja aineistoon tulee suhtautua kriittisesti, koska Internetissä kuka tahansa voi julkaista mitä tahansa tietoa, joka saattaa olla tarkoituksella harhaan johtavaa. Sama koskee myös sähköpostilla ulkopuolelta saapuvia viestejä, koska lähettäjän sähköpostiosoite on helposti väärennettävissä ja erilaisista sähköpostilla tehtävistä huijauksista on olemassa useita vakavia esimerkkejä.

1.3 Kielletyt toiminnot verkossa

Tietoliikenneverkon toiminnan ja tietoturvan takaamiseksi seuraavat toiminnot ovat kiellettyjä:

- palomuurien, virustorjunnan ja vastaavien turvamekanismien kiertäminen tai tietojärjestelmän turvamekanismien tarkoituksellinen ohittaminen;
- työjärjestelmiin liittymättömien vertaisverkko-ohjelmien käyttö muun muassa mahdollisesti tarttuvien haittaohjelmien vuoksi sekä tekijänoikeusrikkomusten ehkäisemiseksi;
- työtehtäviin liittymättömien ohjelmien, musiikki- ja videotiedostojen sekä pelien lataaminen tai tuominen kaupungin tietoverkkoon sekä jakaminen kaupungin verkosta ilman työntekijän lupaa;
- työtehtäviin liittymättömien sivujen, esim. aikuisviihde-, ynnä muiden "vaarallisten" sivujen selailu muun muassa haittaohjelmien vuoksi.

Kaupunki voi rajoittaa teknisillä estoilla Internetissä olevien palvelujen ja www-osoitteiden käyttöä kaupungin verkosta ja laitteilta.

2 Sähköposti

2.1 Määritelmät

Sähköpostiviestit on tässä säännössä jaettu neljään eri luokkaan sen mukaisesti, millaiseen osoitteeseen ne liittyvät.

- organisaation sähköpostiviesti on kaupungin asiointipostiin tullut tai sitä kautta lähetetty viesti, esimerkiksi kirjaamo@kuopio.fi;
- työsähköpostiviesti on työnantajan antamaan sähköpostiosoitteeseen tullut tai sitä kautta lähetetty työtehtäviin liittyvä viesti, esimerkiksi maija.mehilainen@kuopio.fi;
- henkilökohtainen sähköpostiviesti on työnantajan antamaan sähköpostiosoitteeseen tullut tai sitä kautta lähetetty henkilökohtainen eli yksityinen viesti, esimerkiksi maija.mehilainen@kuopio.fi;
- muu sähköpostiviesti on käyttäjän ulkopuoliseen sähköpostiosoitteeseen tullut tai sitä kautta lähetetty viesti, esimerkiksi maija.mehilainen@gmail.com.

2.2 Sähköpostiosoitteen muodostuminen ja julkaiseminen

Sähköpostiosoitteet muodostuvat käyttäjän nimestä. Muotoon etunimi.sukunimi@organisaatio.fi tekevät poikkeuksen samannimiset henkilöt, joiden osoitteisiin lisätään tarvittaessa erotteleva osa. Luonnollisen henkilön sähköpostiosoite on henkilötieto.

Kuopion kaupungilla ja yksiköillä tulee olla organisaation sähköpostiosoitteet virallisten asioiden hoitoa ja palveluiden tarjoamista varten (esimerkiksi kirjaamo@kuopio.fi, yksikko@kuopio.fi). Organisaatio-osoitteen tulee olla selväkielinen, yksiselitteinen ja mahdollisimman lyhyt. Jokaiselle organisaatio-osoitteelle tulee nimetä vähintään yksi vastuuhenkilö, jolla tulee olla myös varahenkilö. Vastuuhenkilö määrittelee sen, miten saapuneet viestit käsitellään ja saataan tiedoksi muille käsittelijöille. Organisaation palveluita tulee lähestyä ensisijaisesti organisaatio-osoitteiden, eikä yksittäisten työntekijöiden sähköpostiosoitteiden kautta.

Julkaisemisella tarkoitetaan sähköpostiosoitteen ilmaisemista esimerkiksi paperijulkaisuissa, julkisilla www-sivuilla ja hakemistopalveluissa. Kaupunki julkaisee organisaatio-osoitteet sekä työntekijöidensä työsähköpostiosoitteet niiltä osin kuin se on tarpeen palveluiden käytön ja tehtävien hoidon kannalta. Henkilökohtaiset sähköpostiosoitteet voidaan julkaista muodossa "etunimi.sukunimi(at)kuopio.fi", tai muulla tavalla selittämällä.

2.3 Sähköpostiin liittyvät rajoitukset ja kiellot

Noudata seuraavia ohjeita sähköpostin käytössä:

- Työsähköpostin välittäminen tai automaattinen ohjaaminen organisaation ulkopuoliseen sähköpostiosoitteeseen on kielletty tietoturvasyistä.
- Jos viestiä ei ole syytä levittää, voi olla hyvä selvästi kirjoittaa viestin alkuun siitä huomautus esimerkiksi "Älä lähetä tätä sähköpostia eteenpäin." Jos kuitenkin ilmenee tarve lähettää viestiä eteenpäin, pyydä lupa jatkolähtämiseen viestin laatijalta.

Kaupungin sähköpostijärjestelmässä on myös mahdollista automaattisen luokittelun (AIP) avulla teknisesti estää viestin jatkolähtäminen. Huomioi, että näiden toimintojen turha käyttö voi hankaloittaa viestin käsittelyä vastaanottajalla.

- Ketjukirjeiden lähettäminen sähköpostilla ei ole sallittua.
- Laajoja, koko henkilöstölle kerralla lähetettäviä sähköpostituksia tulee välttää. Tarve laajan tiedotukseen esimerkiksi tiedotusvastaavien kautta harkitaan tapauskohtaisesti.
- Ennen kuin otat sähköpostikeskusteluun mukaan lisää jäseniä tai lähetät viestejä eteenpäin, varmista, että aiempi viestikeskustelu ei sisällä mitään uudelle vastaanottajalle kuulumatonta sisältöä.

- Organisaatiosähköpostiosoitteisiin (asiointiosoite) saapuneisiin viesteihin työnantajalla on tarvittaessa esteetön pääsy. Näitä sähköpostiosoitteita ei saa käyttää yksityiseen viestintään. Organisaatiopostilaatikoita ei käytetä yhteiskäyttötunnuksilla muulloin kuin erikseen sallituissa perustelluissa poikkeustapauksissa, jolloin tarve kartoitetaan palvelualueen omassa tietohallinnossa.
- Älä tulosta sähköposteja paperille, ellei se ole välttämätöntä. Jos tulostat, niin käytä turva-tulostusta aina kun se on mahdollista.
- Työsähköpostiosoitetta saa käyttää vain sellaiseen verkon palveluihin rekisteröitymiseen, joilla on selkeä yhteys työtehtäviin.
- Ulkopuoliseen sähköpostiosoitteeseen liittyvillä käyttäjätunnuksilla ei saa käyttää samoja salasanoja kuin kaupungin järjestelmien käyttäjätunnuksilla.
- Ulkopuolisen sähköpostiosoitteen ja palvelun käyttö kaupungin tietokoneilla aiheuttaa riskejä sille, että postien mukana tulee haittaohjelmia. Tiedostojen lataamista henkilökohtaisten sähköpostipalveluiden kautta tulee välttää kaupungin tietokoneilla.

Sähköpostitse tehdyt huijaukset ja haittaohjelmaperäiset hyökkäykset ovat lisääntyneet voimakkaasti. Sähköpostijärjestelmän ylläpidolla on oikeus puuttua sähköpostien kulkuun sähköpostijärjestelmän palvelutason tai turvallisuuden takaamiseksi. Kaikkia haitallisia sähköposteja ei saada suodatettua pois. Tästä syystä sähköpostin käyttäjän oma toiminta on erittäin merkittävässä roolissa hyökkäysten ja huijausten torjumisessa.

- Suhtaudu epäluuloisesti tuntemattomalta lähettäjältä saamiisi viesteihin, etenkin jos viestissä on liitteitä tai linkkejä. Huomioi, että tutultakin lähettäjältä voi tulla haittaohjelmia, sillä lähettäjän tiedot on helppo väärentää.
- Mikäli viesti on selkeästi epäilyttävä (olet esimerkiksi voittanut jotain tai saat "ilmaista" rahaa), poista viesti sitä enempää tarkastelematta. Mikäli avasit epäilyttävän viestin ja klikkasit siinä olevaa linkkiä tai avasit viestin liitetiedoston, ota yhteys Istekkiin, vaikka näyttäisi siltä, että mitään ei tapahtunut.
- Kysy viestin lähettäjältä, lähettikö hän viestin tarkoituksella sinulle. Älä kuitenkaan soita etenkään viestissä yhteystietoina annettuihin ulkomaalaisiin numeroihin, mikäli lähettäjä tai numero ei ole sinulle entuudestaan tuttu.

2.4 Asiakkaalta tuleva sähköposti

Sähköisessä asiointissa viranomaisen on viipymättä ilmoitettava kuittausviestillä lähettäjälle sähköisen asiakirjan vastaanottamisesta. Jos lähettäjä pyytää vastausta viestiin, kuittaus lähetetään ilman tarpeetonta viivettä. Kuittausviestin lähettää asiaa käsittelevä henkilö ja automaattikuittauksia tulee käyttää harkiten. Työntekijän lähettämästä työsähköpostiviestistä tulee ilmetä, että sen lähettäjä on viranomainen, ei yksittäinen työntekijä, esimerkiksi liittämällä alikirjoitukseen asema ja yksikön nimi.

Sähköpostiviestejä käsitellään julkisuuslain (621/1999) edellyttämällä tavalla. Julkisuuslaissa säädetään muun muassa, mikä on viranomaisen asiakirja, mitkä ovat salassa pidettävät tiedot ja milloin on oikeus saada tieto asiakirjasta. Sähköiseen asiointiin liittyvät sähköpostiviestit kirjataan, käsitellään ja arkistoidaan tiedonohjaussuunnitelmassa ilmenevällä tavalla.

Mikäli kysymyksessä on hakemus tai muu viranomaistoimenpiteitä edellyttävä toimenpide, tulee paluuosoite asettaa siten tai muistuttaa asiakasta siitä, että jatkoyhteydet hoidetaan organisaatio-osoitteen kautta.

2.5 Sähköpostien rajoittaminen ja suodattaminen

Kuopion kaupunki suojaa sähköpostipalveluaan ja vähentää roskapostiongelmia suodattamalla viestit, jotka saapuvat tunnetuista roskapostia välittävistä palvelimista tai jotka luokitellaan roskapostiksi otsikkotietojensa tai automaattisen sisältöanalyysin perusteella. Esto toteutetaan teknisin menetelmin sähköpostipalvelussa.

Kuopion kaupunki tarkistaa sähköpostiviestit ja niiden liitetiedostot mahdollisten virusten ja muiden haittaohjelmien osalta sekä rajoittaa mahdollisesti haitallisten, viallisten tai liian suurien/monilukuisten liitetiedostojen vastaanottamista ja lähettämistä. Kaupunki poistaa viruksia ja muita haittaohjelmia sisältävät viestit ja liitetiedostot. Kaupungin ei tarvitse tiedottaa yksittäisen viestin suodattamisesta tai tuhoamisesta viestinnän osapuolille tai palauttaa tuhattua viestiä lähettäjälle.

Roskapostiin ei pidä vastata, koska näin vain lisätään roskapostin saapumista. Vastaamalla osoittaa sähköpostiosoitteensa toimivaksi ja se lisätään roskapostittajien jakelulistoille. Jos automaattisesta roskapostien suodattuksesta huolimatta tulee häiritsevässä määrin tunnistamattomia roskapostia tai väärin tunnistettua roskapostia, käyttäjä voi ilmoittaa tästä Istekkiin.

2.6 Perille menemättömät sähköpostiviestit

Sähköpostiviestin lähettäjällä on vastuu viestin luettavuudesta, viestin perillemenosta, mahdollisen määräajan ylittymisestä ja muista näihin verrattavista seikoista, kunnes hän on saanut

tiedon viestin onnistuneesta perillemenosta. Käyttäjien tulee huolehtia, että omassa sähköpostitilaatikossa on riittävästi tilaa uusien sähköpostien vastaanottamiseen ja lähettämiseen.

Mikäli lähetetyn viestin vastaanottajan osoite ei ole sähköpostijärjestelmän tiedossa tai vastaanottajan sähköposti on täynnä, järjestelmä yleensä lähettää viestin lähettäjälle automaattisesti virheilmoituksen. Sähköpostia kirjoittaessa voi Outlookissa halutessaan määrittellä pyydettyväksi vastaanotto- tai lukukuittauksen. Näiden toiminta on kuitenkin riippuvainen vastaanottajan sähköpostijärjestelmästä ja asetuksista.

2.7 Väärään osoitteeseen saapuneet sähköpostiviestit

Mikäli käyttäjä saa toiselle henkilölle tarkoitetun sähköpostiviestin, käyttäjällä on vaitiolovelvollisuus ja hyväksikäyttökielto niin viestin sisällöstä kuin olemassaolostakin. Toiselle henkilölle tarkoitettu sähköpostiviesti on ohjattava edelleen oikeaan osoitteeseen, jos osoite on varmuudella tiedossa. Lisäksi viestin lähettäjää pitää informoida siitä, että viesti on tullut alun perin väärälle vastaanottajalle. Mikäli oikeaa osoitetta ei ole tiedossa, on viestin vastaanottajan lähetettävä alkuperäiselle lähettäjälle tieto epäonnistuneesta toimituksesta ja hävitettävä saapunut viesti.

Organisaation tai virkamiehen toimivaltaan kuulumaton, erehdyksestä tai tietämättömyydestä lähetetty sähköpostiviesti on siirrettävä hallintolain (434/2003) 21 §:n mukaisesti toimivaltaiseksi katsotulle viranomaiselle, jos se on tiedossa. Siirrosta on ilmoitettava viestin lähettäjälle. Ellei siirto ole mahdollinen, viesti palautetaan ja sähköposti poistetaan omasta sähköpostista.

Lähetys- ja palautusvelvollisuudet/ohjeet eivät koske haittaohjelmien lähettämiä viestejä eivätkä roskapostia.

2.8 Palvelussuhteen väliaikainen katkeaminen ja päättyminen

Kun kyse on työntekijän ennakoidusta poissaolosta, on huolehdittava työntekijän sähköpostin asianmukaisesta hoidosta. Suositeltavin tapa on laittaa oman sähköpostin poissaoloviestiin tieto, kelle viestit tulee lähettää poissaolon ajan. Poissaoloviestin voi määrittellä erilaisiksi sisäisille posteille ja ulkoa tuleville posteille. Poissaoloviestien sisältöön tulee kirjata vain olennainen tieto työtehtävien hoitamiseksi poissaolon aikana. Sähköpostijärjestelmän ominaisuuksissa voi myös rajata poissaoloviestin vastaanottajia.

Henkilön käyttöoikeus työnantajan antamaan sähköpostiosoitteeseen päättyy palvelussuhteen päättyessä. Käyttöoikeuksien voimassaolosta vastaa yksikön esimies. Työnantaja sulkee sähköpostiosoitteen työsuhteen päättyessä. Jos työntekijä on lomalla tai estynyt hoitamasta tehtäviään jo ennen työsuhteen päättymistä, esimies voi tapauskohtaisesti käyttää harkintaa sähköpostin käytön keskeyttämisessä tai estämisessä.

Työntekijän yksityiseksi nimeämä kansio hävitetään ja postilaatikkoon jääneet henkilökohtaiset viestit poistetaan. Työhön liittyvät viestit jäävät työnantajan haltuun. Tarvittaessa työnantajalle kuuluvat viestit siirretään esimiehen osoittamalle henkilölle.

Työnantajalla on oikeus lain yksityisyyden suojasta työelämässä (759/2004, 18-20§) asettamissa rajoissa saada käyttöönsä työnantajalle kuuluvat ja sen toiminnan jatkumisen kannalta välttämättömät viestit työntekijän ollessa estyneenä. Työntekijälle lähetettyjen tai tämän lähettämien viestien selville saaminen ja niiden avaaminen perustuu ensisijaisesti työntekijän suostumukseen. Työnantajan oikeudesta hakea esille tai avata työntekijälle lähetettyjä tai tämän lähettämiä sähköpostiviestejä määritellään tarkemmin asiaan liittyvässä erillisessä ohjeessa (kappale 9.2).

2.9 Sähköpostin yksityinen käyttö

Työsähköpostiosoitteen käyttö henkilökohtaisiin tarkoituksiin on luvallista siten, että se ei haittaa kaupungin toimintoja tai työn tekemistä. Käyttö yksityiseen kaupalliseen tarkoitukseen, yritystoimintaan tai poliittiseen mainontaan on kiellettyä. Käyttö henkilökunnan ammattiyhdistysten ja kaupungin oppilaitosten opiskelijajärjestöjen toimintaan on sallittua.

Työnantaja kohtelee työsähköpostiosoitteella toimitettua viestiä pääsääntöisesti vastaanottajalle osoitettuna henkilökohtaisena viestinä, koska vastaanottaja ei voi estää henkilökohtaisten viestien saapumista. Työntekijän henkilökohtaiset viestit tulee erottaa selvästi työsähköposteista. Työntekijän tulee siirtää työsähköpostiosoitteeseensa tulevat henkilökohtaiset viestit omaan kansioonsa, jonka nimi on "Yksityinen". Tämä koskee sekä saapuvia että lähteviä viestejä.

Työnantaja poistaa palvelussuhteen päätyttyä postilaatikkoon jääneet henkilökohtaiset postit. Työnantaja ei ole vastuussa henkilökohtaisten postien tai niiden liiteaineistojen varmistamisesta tai korvausvelvollinen, mikäli kyseiset sähköpostit tai niiden liiteaineistot tuhoutuvat teknisen vian tai häiriön seurauksena tai siksi, ettei niiden säilymistä ole varmistettu.

Organisaation ulkopuolinen sähköpostiosoite eli muu kuin työnantajan tarjoama osoite on yksityisasia, jota ei tässä säännössä tarkemmin ohjata. Työntekijä ei saa käyttää ulkopuolista sähköpostiosoitetta Kuopion kaupungin työtehtäviin ilman työnantajan antamaa lupaa ja hyvää, perusteltua syytä. Työnantaja voi erikseen antaa asiaan kirjallisen luvan, riskit tunnistaen.

2.10 Luottamuksellinen sähköposti

Salassa pidettävät asiakirjat tai muuta luottamuksellista informaatiota sisältävät viestit pitää lähettää aina suojattuina, vaikka vastaanottaja muuta ehdottaisi tai toivoisi. Sähköpostin salauksesta on erillinen ohjeistus kaupungin Intranetissa, tietoturvasivuilla.

Kaupungin ulkopuolelle lähteivissä viesteissä käytetään sec-loppuista turvasähköpostia. Mikäli työntekijä tarvitsee turvasähköpostipalvelua (sec-päätteinen sähköposti), esimies voi tilata turvasähköpostipalvelun työntekijän käyttöön. Turvasähköpostin teknisestä käytöstä on erillinen ohjeistus kaupungin Intranetissa, tietoturvasivuilla.

Kaupungin sisällä (kuopio.fi-osoitteiden välillä) voidaan käyttää Microsoftin omaa sähköpostisalausta tai tietojen automaattista luokittelua eli AIP-suojasta luottamuksellisten sähköpostien lähettämisessä. AIP-palvelu on tarkoitettu sähköpostien ja dokumenttien suojaamiseen ja luokitteluun. Luokittelulla voidaan osoittaa vastaanottajalle, kuinka kyseistä tietoa tulisi käsitellä. AIP:sta on saatavilla erillinen ohje kaupungin Intranetissa.

3 Kaupungin Teamsin ja muiden videoneuvottelusovellusten kokouskäyttö

Teamsin ja muiden videoneuvottelusovellusten kokouskäytössä tulee huomioida seuraavat asiat:

- sovellusten ominaisuuksiin ja käyttöohjeisiin tulee tutustua ennen sovellusten käyttöä;
- osallistuvat henkilöt on varmuudella tunnistettu;
- tiedostetaan, että yksittäisen osallistujan takana voi olla useampi henkilö;
- osallistujilla on oikeus käsitellä tietoa, jota neuvottelussa jaetaan;
- tiedostoja näytetään ja jaetaan vain tarpeellisessa laajuudessa;
- pikaviestimissä oleva chat-keskustelu tallentuu viestihistoriaan;
- keskustelun tallentamisesta tulee sopia erikseen;
- käyttö ammattilaisen ja asiakkaan välisissä neuvotteluissa ohjeistetaan erikseen.

4 Pikaviestinten käyttö

4.1 Tekstiviestit

Tekstiviestillä tarkoitetaan matkapuhelimesta tai tietojärjestelmästä matkapuhelimeen lähetettävää tekstiviestiä eli sms-viestiä.

Viestistä pitää käydä ilmi selvästi kuka ja missä roolissa viestin lähettää. Mikäli asiakkaalle lähetetään salassa pidettäviä tietoja (esim. sosiaali- ja terveydenhuollon asiakastietoja) pitää asiakkaalta pyytää ensin suostumus ja varmistaa matkapuhelinnumero. Asiakas pitää olla tunnistettu. Suostumus pitää kirjata asiakastietojärjestelmään tai liittää muulla tavoin osaksi asiakastietoja.

4.2 Sosiaalisen median viestintävälineet

Kaupunki käyttää sosiaalisen median palveluita (esimerkiksi Facebook, Twitter, Instagram, LinkedIn), viestinnässä ja markkinoinnissa. Sosiaalisen median palveluissa saa käsitellä vain julkista tietoa. Kuopion kaupunki ei osallistu väittelyihin eikä ota kantaa mahdollisiin omiin tai muiden ristiriitatilanteisiin. Provokatiivisiin Kuopion kaupungille osoitettuihin viesteihin ei reagoida. Laittomat, siveettömät, aggressiiviset sekä loukkaavat viestit poistetaan omassa hallinnassa olevista palvelusta siitä erikseen tiedottamatta.

Kaikessa viestinnässä tulee noudattaa organisaation omia viestintäohjeita. Lisäksi on huomioitava,

- mitä työnantajan tietoja julkaistaan
- kuka omistaa ja vastaa julkaistuista tiedoista
- muodostuuko rekistereiksi luokiteltavia tietoja
- miten henkilötietojen suoja toteutuu
- vuotaako työnantajan salassa pidettäviä asioita nettiin

Sosiaalisen median viestintävälineitä ei saa käyttää toisten henkilöiden yksityisyyttä kuvaavien tietojen eikä salassa pidettävien tietojen välittämiseen. Sama koskee myös erilaisia asiakaspalveluun liittyviä keskusteluvälineitä kuten chat:ia, joissa voidaan antaa ohjausta yleisellä tasolla, mutta ei käsitellä arkaluonteisia henkilötietoja tai salassa pidettäviä tietoja.

Älä sokeasti luota sosiaalisen median kautta tuleviin viesteihin, sillä sosiaalisessa mediassa on helppo tehdä toisten nimissä tunnuksia tai kaapata toisen henkilön sähköinen identiteetti. Yhteisöpalveluja käytetään usein myös tahallisesti virus-, haitta- ja vakoiluohjelmien levityskanavana. Uhkana ei sinällään ole itse palvelu, vaan siellä jaettavat linkit, joita kannattaa varoa. Lisäksi usein toimitaan Suomen lakien ulottumattomissa.

Somen käytöstä on kaupungilla erilliset ohjeet, jotka löytyvät kaupungin intranetistä, markkinoinnin ja viestinnän sivuilla

4.3 Pikaviestimet

Palveluiden turvallisuus ja luotettavuus vaihtelee hyvin paljon ja vaikuttaa merkittävästi siihen, mihin tarkoituksiin kyseistä palvelua voi käyttää. Monet ilmaiset pikaviestimet ovat verrattavissa tietoturva- ja tietosuojamielessä sosiaalisen median palveluihin.

Pikaviestinten (esim. WhatsApp, Signal, Telegram, tai vastaava.) käytössä on tärkeää huomioida, onko palvelun käyttämä yhteys salattu sekä minne ja miten tiedot tallennetaan. Oleellista on myös se, kenellä on järjestelmään syötettyjen tietojen omistus- ja/tai käyttöoikeus sekä kenelle tiedot näkyvät tai kuka niitä pääsee katsomaan.

Tärkeää on tutustua kyseisen palvelun käyttöehtoihin, esimerkiksi sallitaanko työkäyttö ja mitä

se maksaa, sekä palvelun tietosuojaan, esimerkiksi miten käyttäjän tietoja suojataan, käytetään tai luovutetaan. Se, että joku palvelu on jo käytössä jossain muussa organisaatiossa ei vielä takaa sitä, että se olisi laillinen, turvallinen tai järkevä käyttää.

Kaupungin tietoturva- ja tietosuojaryhmä on tunnistanut seuraavanlaisia riskejä ilmaisten pikaviestimien käytössä:

- Ilmaisversioissa ei yleensä ole mahdollista solmia organisaatiokohtaista GDPR:n (28 artikla) edellyttämää sopimusta, jossa sovittaisiin rekisterinpitäjän ja käsittelijän vastuista. Kaupungilla ei siten ole keinoja määritellä sitä, missä ja miten tietoja käsitellään.
- Käyttämällä väärä asetuksia, voi joissakin tapauksissa koko keskusteluhistoria päätyä salaamattomana ulkomaisille palvelimille ja niitä voidaan hyödyntää esimerkiksi käyttäjien profilointiin sekä markkinointitarkoituksiin.
- Erilaisissa pikaviestimien keskusteluryhmissä kertyvät tiedot eivät ole käyttäjän itsensä, saati organisaation, hallittavissa tai valvottavissa. Organisaatio / rekisterinpitäjä ei välttämättä edes tiedä keskustelujen olemassaolosta. Kaupungilla ei ole mahdollisuutta vaikuttaa henkilötietojen osalta GDPR:n vaatimusten toteuttamiseen eikä taata henkilöille heidän tietoaan koskevia GDPR:n mukaisia oikeuksia. Kaupungilla ei ole myöskään mahdollisuuksia varmistaa muun salassa pidettävän tiedon asianmukaista käsittelyä ilmaisissa pikaviestinpalveluissa.

Ilmaiset verkosta saatavat pikaviestinpalvelut eivät sovellu salassa pidettävän tiedon käsitteilyyn tai henkilötietojen käsittelyyn asiakastyössä.

5 Sähköisen kalenterin käyttö

Kokouksiin tulee ensisijaisesti esittää kutsut sähköisinä kalenterikutsuina. Salassa pidettävää aineistoa ei pidä liittää kalenterikutsuun. Esimerkiksi otsikko näkyy kalenterissa kaikille, asetuksista riippuen.

Kalenterimerkinnöissä on muistettava tietosuoja. Outlookin kalentereihin ei saa tallentaa salassa pidettäviä henkilötietoja, koska kyseessä ei ole asiakastietojärjestelmä. Ajanvaraukset tulee tallentaa potilas-/asiakastietojärjestelmiin.

Kalenteri voidaan halutessa jakaa avoimeksi kaikille tai määritellyille työntekijöille tai työntekijäryhmille. Tällöin kaikki merkinnät, jotka eivät ole yksityisiä, ovat näkyvissä jaetun kalenterin katselijoille. Kalenterin jaon yhteydessä voi määritellä sen, mitä toiset työntekijät voivat kalenterilla tehdä tai siitä nähdä.

6 Tilanvarauskäytännöt

Henkilökunnan käyttöön tarkoitettujen kokoustilojen varaukset tulee tehdä Outlookin kalenterilla. Jokainen pystyy tekemään varauspyyntöjä tilakalentereihin omaan kalenteriin tekemänsä kalenterikutsun kautta. Varauksista tulee sähköpostiin kuittaus siitä, onko varaus onnistunut tai hylätty. Varauksia tulee tehdä vain tiloihin, joihin on itsellä kulkuoikeus tai muuten sovittu tilan haltijan kanssa pääsystä.

Kokoustilat tulee nimetä yhdenmukaisesti, loogisesti ja helposti löydettäviksi toimipaikan nimen perusteella. Varausta ei saa tehdä suoraan neuvotteluhuoneen tai resurssin kalenteriin kuin poikkeustapauksissa.

7 Pilvestä käytettävät palvelut

7.1 Maksulliset palvelut

Työtehtävissä on käytettävä työnantajan hankkimia palveluita, jotka toimivat Kuopion kaupungin työympäristössä. Mikäli Kuopion kaupungin työympäristössä ei ole tarkoitusta vastaavaa palvelua, on mahdollista joissakin tapauksissa hyödyntää myös maksullisia pilvestä käytettäviä palveluja. Näiden käyttöönottoon kuitenkin liittyy riskejä, minkä vuoksi hankinta ja käyttöönotto täytyy tehdä hallitusti ja sopimuksellisesti, sekä niihin tarvitaan työnantajan lupa.

Pilvestä käytettäviin palveluihin liittyy samoja vaatimuksia kuin perinteisiin tietotekniikan sovelluksiin, ja niiden yhteydessä täytyy ottaa huomioon Kuopion kaupungin muu ympäristö, sopimukset ja lainsäädäntö.

7.2 Ilmaispalvelut

Verkossa on saatavilla laaja kirjo erilaisia, eri tarkoitukseen käytettäviä palveluja, jotka näennäisesti ovat "ilmaisia". Näiden palvelujen maksuttomuus perustuu lähes aina siihen, että käyttäjän tietoja ja verkkoselaushistoriaa kyseisessä palvelussa kaupataan eteenpäin muille tahoille ja yhteistyökumppaneille, muun muassa mainostajille.

Ongelmia aiheutuu muun muassa ylläpidon puuttumisesta. Tieto ei ole saatavilla esimerkiksi tapauksessa, jossa tiedot tallentanut työntekijä on estynyt käyttämään palvelua. Ongelmia saattaa ilmaantua myös esimerkiksi lokituksiin liittyvissä asioissa. Käyttäjällä ei ole mahdollisuutta päästä lokitietoihin käsiksi eikä kaupunki voi selvittää ongelmatilanteita lokitietojen perusteella, kuten kaupungin omissa palveluissa. Palveluntarjoajat keräävät yleensä paljon tietoa palvelun käytöstä, sinne tallennetusta materiaalista ja sen käyttäjistä, eikä lokien käyttö välttämättä ole tietosuojalainsäädännön mukaista.

Kaupungin sähköpostilla rekisteröityminen yleensäkin netin ilmaisiin palveluihin on tehtävä erittäin harkiten. Työsähköpostiosoitetta saa käyttää vain sellaiseen verkon palveluihin rekisteröitymiseen, joilla on selkeä yhteys työtehtäviin.

7.3 Yhteys tietohallintoon

Ota aina yhteyttä oman palvelualueesi tietohallintoon, jos pilvipalvelun käyttöön liittyy

- henkilötietojen käsittelyä
- salassa pidettävän materiaalin käsittelyä
- pankkitietojen käsittelyä
- ylläpitovaatimuksia
- 24/7-käytettävyyksivaatimuksia
- lisenssejä
- kustannuksia
- suuria käyttäjämääriä
- useita yksiköitä
- poikkeusoloissa tarvittavia tietoja

8 Käytön valvonta sekä lokitietojen kerääminen ja säilyttäminen

Sähköisten välineiden käytöstä tallentuu erilaisia lokitietoja käyttäjän työasemaan, työnantajan palvelimille sekä Internetissä toimivien operaattoreiden ja palveluntarjoajien palvelimille.

Esimerkiksi Internet-selailun yhteydessä lokitiedoilla tarkoitetaan tietoja siitä, milloin ja minne käyttäjä on ottanut yhteyden. Internet-liikennettä voidaan seurata tilastollisesti ainoastaan siten, että valvonta ei kytkeydy yksittäiseen käyttäjään. Lokitietoja kerätään automaattisesti ja niitä käytetään tekniseen kehittämiseen sekä virhetilanteiden ja mahdollisten väärinkäytösten selvittämiseen.

Työasemiin ja verkon välimuistipalvelimiin voi tallentua myös kokonaisia www-sivuja, joita käyttäjä on selannut. Sivujen tai yhteystietojen säilytysaika työasemilla riippuu muun muassa selaimen asetuksista. Käyttäjän tulee ottaa huomioon, että saman koneen muut käyttäjät voivat päästä käsiksi näihin tietoihin. Käyttäjä voi itse poistaa työasemaan tallentuvia tietoja selaimen valikoiden kautta.

Internetin palveluissa ja ulkopuolissa www-sivustoissa ei saa käyttää samoja salasanoja kuin työnantajan järjestelmissä. Internet-selaimet mahdollistavat www-sivuihin liittyvien salasanojen tallentamisen selaimen muistiin. Tämän toiminnon käyttöä ei suositella tietoturva- ja tietosuojasyistä etenkin, jos kone on useamman henkilön käytettävissä.

9 Näiden sääntöjen valvonta

9.1 Yleiset periaatteet

Näiden sääntöjen valvonnasta vastaavat kaupungin esimiehet, tietohallinto sekä ICT-palvelusta vastaava taho. Mikäli sähköisten viestintävälineiden käyttäjä havaitsee näiden sääntöjen vastaista menettelyä omassa tai muiden toiminnassa, tulee siitä viivytyksettä ilmoittaa omalle esimiehelle ja/tai tietohallinnolle. Jokaisen tulee myös ilmoittaa havaitsemistaan tietoturvaan ja tietosuojaan liittyvistä puutteista, väärinkäytöksistä tai niiden epäilyistä esimiehelle ja/tai tietohallintoon. Tietoturvan ja tietosuojan rikkoutuessa toimitaan erillisen ohjeen mukaan (kapale 9.2).

Jos henkilö toimii vastoin näitä sääntöjä, työnantaja voi ryhtyä tarvittaviin työoikeudellisiin ja rikosoikeudellisiin toimenpiteisiin ja vaatia vahingonkorvauksia. Tietoturvarikkomuksien arvioinnista ohjeistetaan erikseen (kpl 9.2)

Nämä säännöt päivitetään tarvittaessa. Päivitystarvetta seuraa kaupungin Tietoturva- ja tietosuojaryhmä. Tätä dokumenttia voidaan päivittää ilman erillistä hyväksyntämenettelyä silloin, kun kyseessä on organisaatiomuutoksesta, lakimuutoksesta tai muusta vastaavasta muutoksesta aiheutuva tekninen tarve päivitykselle.

9.2 Kuopion kaupungin tietoturva- ja tietosuojalinjaukset ja ohjeet

Linjaukset ja säännöt:

- Tietoturva- ja tietosuojapolitiikka
- Sähköisten viestintäpalveluiden käyttösäännöt
- Käyttövaltuuspolitiikka
- Lokienhallinnan politiikka
- Tietoturvapoikkeamien käsittelysääntö
- Työntekijän sähköpostin ja työtiedostojen hakeminen poikkeustilanteessa
- Tietoturvarikkomusten tulkinta- ja seuraamussäännöstö

Ohjeet:

- Tietojen ja tietojärjestelmien käyttö- ja salassapitositoumus
- Käyttäjän tietoturvaohje
- Tiedonhallinnan pelikirja
- Asiakirjajulkisuus ja tietojen luovuttaminen, yleinen ohje
- Tietoturvapoikkeamat ja toiminta poikkeustilanteissa
- Henkilötietopyyntöjen käsittely
- Virustorjuntaohjelman käyttöohje
- Salattu sähköposti - käyttöohje

10 Keskeisiä lakeja

- EU:n yleinen tietosuoja-asetus (GDPR) 679/2016
- Tietosuojalaki 1050/2018
- Laki viranomaisen toiminnan julkisuudesta 621/1999
- Laki julkisen hallinnon tiedonhallinnasta 906/2019
- Laki yksityisyyden suojasta työelämässä 759/2004
- Laki sähköisen viestinnän palveluista 917/2014

11 Sanasto

TEPA-termipankki: <http://www.tsk.fi/tsk/termitalkoot/>