CPD*Lab*

Continuing Professional Development *Lab*

CPD*Lab*-kurssi: Digitaalinen turvallisuus Kouluttajan opas

Digitaalisten työkalujen turvallinen ja asianmukainen opetus- ja oppimiskäyttö, parannettu turvallisuusohjeistus perusopetuksen yläluokille, virtuaaliseen kiusaamiseen puuttuminen, verkkoyhteisöpalvelujen käyttö, mobiiliteknologian ja Internetin vastuullinen käyttö

Päivämäärä: syyskuu 2013

European Schoolnet

Indire
Istituto Nazionale di Documentazione, Innovazione e Ricerca Educativa

direção-geral da educação

THE NORWEGIAN CENTRE FOR ICT IN EDUCATION

FINNISH NATIONAL BOARD OF EDUCATION

UNIVERSITY of OULU
OULUN YLIOPISTO

Lifelong Learning Programme

CPD*Lab*-projekti on osittain Euroopan komission Elinikäisen oppimisen ohjelman (Lifelong Learning Programme) rahoittama

Sisällysluettelo

CPD*LAB*: DIGITAALISEN TURVALLISUUDEN KURSSI

Johdanto

Digitaalinen turvallisuus: Digitaalisten työkalujen turvallinen ja asianmukainen opetus- ja oppimiskäyttö, parannettu turvallisuusohjeistus perusopetuksen yläluokille, virtuaaliseen kiusaamiseen puuttuminen, verkkoyhteisöpalvelujen käyttö, mobiiliteknologian ja Internetin vastuullinen käyttö oppimisessa, työssä ja elämässä.

CPD*Lab*-kurssin runko ja moduulit perustuvat aiempaa koulutusmateriaalia koskevan kyselyn pohjalta saatuun tietoon ja EUN:in Insafe-ohjelman ja osallistujamaiden asiantuntemukseen sekä EU Kids online -verkoston tutkimukseen. Saatujen vastausten ja tietojen pohjalta todettiin, että vaikka digitaalisesta turvallisuudesta on saatavilla runsaasti tietoa, siihen liittyvää koulutusta ei ole riittävästi tarjolla. Tämä puute nähtiin tärkeäksi paikata.

Digitaalista turvallisuutta käsittelevän koulutuksen tavoitteena on yhdistää nykyinen olemassa oleva tieto ja asiantuntemus kurssiksi, joka perustuu asiantuntijatietoon, tapaustutkimuksiin, käytännön harjoituksiin sekä erilaisten hyvien tietolähteiden löytämiseen ja linkittämiseen.

Tässä asiakirjassa kuvattujen moduulien laatimisessa on käytetty kurssisuunnittelupohjaa, joka on CPD*Lab*-projektikumppaneiden ja pedagogisen neuvottelukunnan (Pedagogical Advisory Board) hyväksymä. Pohja on osa kurssinsuunnitteluasiakirjaa (Course Development Specification), jossa määritetään CPD*Lab*-kurssien kehittämisen periaatteet. Kyseistä pohjaa käytetään kaikilla kolmella CPD*Lab*-kurssilla.

Kurssin ja sen osioiden kehittämisvälineenä on käytetty jatkuvaa arviointiprosessia, kuten projektin hyväksyntäkäytännöissä ja laadunvarmistusprosesseissa määritetään. Osallisina prosessissa ovat projektikumppanit, aihealueiden asiantuntijat ja opettajat, ja sitä ohjaa projektin pedagoginen neuvottelukunta.

Kurssisuunnittelun määritelmät

Kurssin määrittely	CPD*Lab*-projektin kurssisuunnittelumallin taustalla olevat sovitut tavoitteet ja periaatteet ohjaavat kurssin suunnittelua.
Kohderyhmä ja kurssin vaikeustaso	Kurssiasiakirjat kirjoitetaan kurssia pitävälle kouluttajalle. Kouluttajat ovat kurssin aihepiirin asiantuntijoita. Kurssi on vaikeustasoltaan sellainen, että opettajat pystyvät seuraamaan kurssin opetusta kouluttajan johdolla. CPD*Lab*-projektin kohderyhmänä olivat vuosiluokkien 5–9 opettajat. Opettajille suunnatun kurssisisällön näkökulma on pedagoginen. Joissain kohdissa saatetaan antaa sisältöä tukevaa koulutusta tekniikan käyttöön, mutta kurssi itsessään ei keskity tekniikan opetukseen. Osallistujilta odotetaan perustaitoja tieto- ja viestintätekniikan käytössä. Opettajien kouluttaja antaa tukea teknisissä kysymyksissä.
Kouluttajan opas	Kouluttajan opas sisältää kurssisuunnitelman. Se on yksittäinen asiakirja, joka sisältää kurssin rungon ja kaikki kurssin moduulit. Kyseinen asiakirja on tarkoitettu kurssin toteuttamisesta vastaavalle kouluttajalle. Siihen sisältyy kurssin yleiskuvaus (runko), ohjeet kurssin pitämiseen, kurssin moduulit, viitteet tukimateriaaliin sekä kurssitehtävät. Moduulien tukimateriaalit koostuvat useista asiakirjoista, joita käytetään tehtävien tekemisessä.
Kurssin runko	Runko antaa kouluttajalle yleiskuvan kurssista. Se sisältää visuaalisen yleiskuvauksen kurssista ja tietoa vaihtoehtoisista tavoista sen toteuttamiseksi. Nämä eri vaihtoehdot auttavat kouluttajaa arvioimaan ja tekemään päätöksen siitä, miten kurssi palvelee parhaiten paikallisia tarpeita ja olosuhteita.
Kurssimoduuli	Kurssi koostuu kymmenestä eri moduulista. CPD*Lab*-projektin kurssisuunnittelun vuoksi kokonaisuus suunniteltiin pidettäväksi viisi päivää kestävänä ja lähiopetuksena annettavana koulutuskurssina, joka täyttää Comenius-ohjelman ehdot opettajien täydennyskoulutusapurahoille. Kurssimoduulit ovat yleensä puoli päivää (3 tuntia) kestäviä kokonaisuuksia, joihin kuuluu erilaisia tehtäviä. Viisi päivää kestävä kurssi käsittää siis yhteensä kymmenen moduulia. Moduulit on suunniteltu toteutettavaksi joko yksittäin tai useamman moduulin yhdistelmänä. Näin kansallisella/paikallisella tasolla voidaan valita joustavasti joko kaikki tai osa moduuleista, paikallisten tarpeiden mukaan. Tämä tarkoittaa sitä, että vaikka kurssi on suunniteltu viisipäiväiseksi koulutukseksi, jossa moduulit muodostavat yhtenäisesti etenevän kokonaisuuden, se on myös joustava. Moduuleista on mahdollista tehdä erilaisia yhdistelmiä, jolloin kansalliset kouluttajat voivat räätälöidä osanottajien tarpeiden mukaan kaksi- tai kolmipäiväisen kurssin.

Kurssitehtävä	Jokainen moduuli jakautuu kurssitehtäviin. Kurssitehtävä tarkoittaa aktiviteettia, johon kurssin osanottajat osallistuvat. Jokainen moduuli sisältää erilaisia tehtäviä, esimerkiksi: • itsensä esittely • aineistoihin tutustuminen (videot, linkit verkkoaineistoihin jne.) • työskentely tapaustutkimuksen parissa • tehdyn työn pohdiskelu • moduulin/kurssin arviointi. Joissain tehtävissä voidaan valita useasta eri vaihtoehdosta. Kouluttaja voi valita vapaasti kurssin osallistujien kanssa toteutettavat tehtävät ja niille sopivan aikataulun.
Kurssin tukimateriaali	Kurssin tehtäviin liittyy useita tukimateriaaleja, joita käytetään kussakin moduulissa kouluttajan oppaan mukaisesti. Niihin viitataan tässä oppaassa nimellä "kurssin tukimateriaali". Tukimateriaalit on tallennettu erikseen ja ne ovat saatavilla yksittäin. Kurssin tukimateriaali auttaa kouluttajaa toteuttamaan kurssin kokonaisuudessaan. Kokeneilla kouluttajilla voi kuitenkin olla käytössään myös omaa tukimateriaalia opetuksen tueksi. Näissä tapauksissa kurssin joustava rakenne mahdollistaa sen, että kouluttaja voi vaihtaa materiaaleja paremmin paikalliselle yleisölle sopivaksi ja/tai ottaa mukaan paikallista kontekstia, kansallisilla kielillä olevaa materiaalia tai ajankohtaisempia esimerkkejä.

Digitaalisen turvallisuuden kurssi: Tekijät ja kiitokset

Digitaalisen turvallisuuden kurssin kehittämistä on johtanut yksi CPD*Lab*-projektikumppaneista, Suomen Opetushallitus (OPH).

Tämä kurssi on useiden ihmisten ahkeran työn ja sitoutumisen tulosta. Erityiskiitos kuuluu seuraaville henkilöille:

- Jukka Tulivuori johti CPD*Lab*-projektin digitaalisen turvallisuuden kurssin kehittämistyötä OPH:n edustajana. Hänen apunaan toimivat Tina Heino, Elisa Helin ja Ella Kiesi.
- Päätekijät, ICT CPD -konsultti Gráinne Walsh ja Insafe-verkoston oma konsultti Karl Hopwood, toivat projektiin käytännön kokemuksensa Euroopan komission Insafe-verkoston kautta. Yhdessä he auttoivat meitä luomaan kurssin, joka on hyvin käytännönläheinen ja hyödyksi sekä opettajille että TVT-koordinaattoreille ja koulun johdolle.
- Kurssin arvioijat, mm. Insafe-verkoston johtaja Janice Richardson yhdessä CPDLab-projektikumppaneiden kanssa, pedagogisen neuvottelukunnan jäsenet, sekä viimeisenä mutta ei vähäisimpänä, jokaista projektikumppania edustavat asiantuntijaopettajat, jotka tukivat kehitystyötä validoimalla ja pilotoimalla kurssia omissa kouluissaan ja luokissaan.

Toivomme, että pidätte kurssista ja siitä on teille paljon hyötyä.

Syyskuu 2013

DIGITAALISEN TURVALLISUUDEN KURSSIN RUNKO

Kurssin nimi:	Digitaalinen turvallisuus: turvallisempi koulu ja luokkaympäristö
Tekijä	Gráinne Walsh
Päivämäärä	5.8.2013
Versionumero	5.3
Tiedoksi kouluttajille	Useimpiin moduuleihin sisältyy PowerPoint-esityksiä. Niiden päätarkoitus on koota yhteen paikkaan kouluttajan saataville kurssin sisällöt, linkit, tehtävät ja videot. Jokaiseen esitykseen on sisällytetty taukoja, jotka on tarkoitettu videoiden katsomiseen, keskusteluun, pienempiin ryhmiin jakautumiseen, käytännön harjoituksiin ja esittelyihin. Vaikka PowerPoint-esitykset sisältyvät moduuleihin, niiden käyttö ei ole pakollista. Paikalliset kouluttajat, jotka vetävät kurssin tai osia siitä, voivat muokata ja päivittää sisältöä koulutukseen osallistujille sopivaksi haluamallaan tavalla. Koska Internetin sisältö muuttuu jatkuvasti, linkit eivät pysy samana. Kouluttajien tulee tarkistaa linkit ennen käyttöä sekä lisätä paikallisia ja ajantasaisempia linkkejä tarpeen mukaan, jotta kurssi pysyy ajankohtaisena. Kouluttajien on osattava käyttää ja auttaa osallistujia käyttämään interaktiivisia yhteistoiminnallisia työkaluja, kuten sosiaalisia kirjanmerkkipalveluja, keskustelufoorumeja ja Twitteriä. On tärkeää, että osallistujia opastetaan käyttämään näitä digitaalisia työkaluja turvallisesti. Näin voidaan hälventää pelkoja, joita niiden käyttöön liittyy. Kun osallistujat oppivat kurssin aikana, miten sosiaalisen median työkaluilla voidaan tehostaa opetusta ja oppimista, he voivat auttaa oppilaitaan kehittämään lukutaitoaan ja käyttämään Internetiä turvallisesti ja eettisesti oppimisessa, työssä ja muilla elämänaloilla. Olennaista on, että ryhmällä on kurssin aikana käytössä jaettu verkko-oppimisympäristö, jotta osanottajat voivat jakaa aineistoja ja hyödyntää Internetin tarjoamia mahdollisuuksia sekä saada tukea aktiiviselle oppimiselle. Paikallisten kouluttajien tulisi harkita yhteisen verkko-oppimisympäristön perustamista ryhmälle (esim. Moodle, Schoology). Tarkoituksena on jakaa kurssin sisältöä tukevia aineistoja sekä tarjota osallistujille keskustelufoorumi ja alue oppimisen tukemista varten. Oppimisalusta rohkaisee osallistujia aktiiviseen, osallistavaan ja sosiaaliseen oppimiseen sekä omien aineistojen jakamiseen.
Johdanto	Eräs koulujen keskeisistä haasteista on Web 2.0 -teknologioiden käyttöönotto sekä mobiiliteknologian, Internetin ja sosiaalisen median lisääntyvä käyttö koulutuksessa. Koulut ovat kiinnostuneita selvittämään uusien, luovien ja yhteistoiminnallisten digitaalisten teknologioiden käytön mahdollisuuksia opetuksessa ja oppimisessa. Toisaalta opettajat ja oppilaat saattavat myös kokea verkkomaailman häm-

	mentävänä. On hankalaa tietää, kuinka käyttää palveluja turvallisesti ja samalla hyödyntää täysimittaisesti kaikki Internetin tarjoamat mahdollisuudet oppimisessa ja muilla elämänalueilla. Nuoria täytyy auttaa kehittämään digitaalista lukutaitoaan ja heille täytyy antaa mahdollisuuksia kehittää ja harjoitella digikansalaistaitojaan. Myös opettajat tarvitsevat enemmän tietoa ja asiantuntemusta voidakseen tukea ja opettaa nuoria käyttämään digitaalisia työkaluja ja laitteita sekä verkkoa turvallisesti. Opettajien täytyy lisäksi tietää, kuinka huolehtia omasta yksityisyyden suojastaan sekä hallita virtuaalisen ja fyysisen luokkaympäristön sisältämiä riskejä ja uusia työkaluja, jotka voivat aiheuttaa haittaa oppilaan omalle tai muiden turvallisuudelle tai yksityisyydelle. Nuoret oppivat Internetin ja sosiaalisen median turvallista ja vastuullista käyttöä sekä opettajilta että vanhemmiltaan. Digitaalisen turvallisuuden kurssi on tarkoitettu turvallisen oppimisympäristön kehittämiseen kouluissa. Kurssilla pyritään edistämään verkon turvallista käyttöä, digitaalista lukutaitoa ja digikansalaisuutta. Kurssin sisältö liittyy suoraan digitaalisen turvallisuuden kysymyksiin, joita opettajat kohtaavat luokkaympäristössä. Se auttaa kehittämään koko koululle asteittain etenevän digitaalisen turvallisuuden opetussuunnitelman, joka on keskeinen osa koulun digitaalisen turvallisuuden ohjelmaa.
Yleiskuvaus	Kurssi auttaa nuorten kanssa työskenteleviä kehittämään digitaaliseen turvallisuuteen ja digimaailmaan liittyvää osaamistaan. Se auttaa heitä myös tukemaan oppilaita ja koulua yhteistoiminnallisten digitaalisten työkalujen käytössä. Keskiössä ovat pedagogiset strategiat ja lähestymistavat, joilla voidaan tukea nuoria tasapainottamaan digitaalimaailman tarjoamia mahdollisuuksia ja sen riskejä. Viisipäiväistä lähiopetuksena tarjottavaa kurssia vetävät digitaalisen turvallisuuden asiantuntijat. Kurssin sisältönä on digitaalisen median käyttö pedagogisiin tarkoituksiin, sosiaalisen median työkalujen soveltaminen opetuksessa ja oppimisessa, käytännön aktiviteetit ja ryhmätyöt. Kurssi on rakenteeltaan modulaarinen ja se perustuu Euroopan komission Insafe-verkoston tekemään tutkimukseen ja materiaaleihin, jäsenmaiden Safer Internet Centre -hankkeiden työhön, EU Kids Online -verkoston tutkimukseen ja kansainvälisiin digitaalisen turvallisuuden verkostoihin, jotka auttavat suojaamaan lapsia ja nuoria Internetin ja mobiililaitteiden käytössä. Osallistujat oppivat vähentämään yleisimpiä lapsiin ja nuoriin kohdistuvia verkkoriskejä ja kehittämään lasten ja nuorten digitaalista lukutaitoa ja digikansalaistaitoja. He harjoittelevat sisällyttämään digitaalisen turvallisuuden parhaita käytäntöjä oppituntien suunnitteluun ja luomaan koko koulun kattavan digitaalisen turvallisuuden opetussuunnitelman. Osallistujat pääsevät kehittämään digitaaliseen turvallisuuteen liittyviä taitojaan ja tutustuvat monenlaisiin materiaaleihin, joita voi hyödyntää opetuksessa ja oppimisessa. Kurssilla perehdytään oppilaiden digitaalisen osaamisen kehittämiseen ja siihen, kuinka soveltaa par-

	haita digitaalisen turvallisuuden käytäntöjä luokkaympäristössä ja koko koulussa. Lisäksi tarkastellaan digitaaliseen turvallisuuteen liittyvien ongelmatapausten käsittelyä. Osallistujat pääsevät käyttämään sosiaalisen median työkaluja, kuten sosiaalisia kirjanmerkkejä ja Twitteriä, sekä interaktiivisia ympäristöjä, kuten blogeja ja keskustelufoorumeita. Näin he saavat tietoja ja taitoja, joista on hyötyä sekä opetuksessa että ammatillisessa kehittymisessä. Kurssilla tarkastellaan yksityiselämään ja työhön liittyviä turvallisuuskysymyksiä. Lisäksi osallistujat pohtivat, kuinka jakaa uutta tietoa muille kollegoille kouluissa. Osallistujat arvioivat koulunsa digitaalisen turvallisuuden opetuksen eSafety Label -työkalun avulla ja suunnittelevat, kuinka digitaalisen turvallisuuden käytännöt saataisiin juurrutettua osaksi koko koulun toimintaa. Näin osallistujat oppivat kehittämään koko koulun kattavan digitaalisen turvallisuuden ohjelman.
Edellytykset osallistumiselle	Viisipäiväinen kurssi on suunniteltu pidettäväksi Future Classroom Lab -koulutustiloissa Brysselissä. Kurssille voivat osallistua opettajat, kouluttajien kouluttajat ja koulujen johtajat tai johtotason toimijat, jotka vastaavat CPD-ohjelmien toteuttamisesta kansallisella tai paikallisella tasolla. Modulaarisen rakenteen ansiosta tulevat paikalliskouluttajat pystyvät muokkaamaan koulutuskokonaisuudet sopiviksi erilaisille kohderyhmille, kuten opettajille, koulujen johtajille ja päättäjille. Osallistujilla tulee olla perustaidot tieto- ja viestintätekniikan käytössä ja heidän tulee olla kiinnostuneita digitaalisen mediateknologian ja Internetin opetus- ja oppimiskäytöstä.
Kurssin tavoitteet	Kurssin suorittamisen jälkeen osallistujat • osaavat määritellä digitaalisen turvallisuuden ja siihen liittyvät parhaat käytännöt • ymmärtävät, että koko koulun kattava digitaalisen turvallisuuden ohjelma on paras tapa turvata kouluyhteisö ja tarjota turvallinen oppimisympäristö • osaavat auttaa oppilaita käyttämään Internetiä ja opetusta sekä oppimista tehostavia digitaalisia työkaluja turvallisesti ja vastuullisesti • osaavat tehostaa opetusta ja oppimista digitaaliseen turvallisuuteen liittyvien taitojensa ja osaamisensa avulla • osaavat vähentää digitaaliseen turvallisuuteen liittyviä riskejä sekä luokkaympäristössä että sen ulkopuolella uusien tietojensa ja taitojensa avulla • osaavat arvioida digitaaliseen turvallisuuteen liittyviä työkaluja ja materiaaleja, joita voi hyödyntää opetuksessa ja oppimisessa ja jakaa kollegojen kanssa • osaavat luoda strategioita, joilla voi suojata itseään verkossa • voivat jakaa ideoita, uutta tietoa ja pedagogisia metodeja kollego-

	jensa kanssa kouluissa esimerkiksi vertaisoppimisen kautta, jotta digitaalinen turvallisuus ja lukutaito saadaan nivottua opetussuunnitelmaan • osaavat luoda koululle digitaalisen turvallisuuden strategian, jolla digitaalinen turvallisuus sisällytetään koko koulun opetussuunnitelmaan • voivat jakaa koko koulun kattavia strategioita digitaalisen turvallisuuden ohjelman kehittämiseksi koko koululle.
Koulutuspäivien ohjelma	Kurssin koko ohjelma on nähtävissä alla.
Vaihtoehtoisia tapoja kurssin toteuttamiseen	Kurssi on suunniteltu viisipäiväiseksi, ja se suositellaan pidettäväksi sellaisena. Kurssin moduulirakenteen ansiosta sitä voi kuitenkin halutessaan muokata eri kohderyhmille sopivaksi, esimerkiksi opettajille tai rehtoreille ja koulun johtajille. Ehdotuksia vaihtoehtoisiksi toteuttamistavoiksi: **Iltaisin tai lauantaisin järjestettävä modulaarinen kurssi** **(6 viikkoa – 2,5 tuntia kerrallaan)** Moduuli 1 Digitaalinen turvallisuus koulussa ja luokassa Moduuli 2 Digitaalista turvallisuutta nuorille ja opettajille Moduuli 3 Digitaalinen turvallisuus: digitaalinen kansalaisuus Moduuli 5 Digitaalinen turvallisuus: digitaalinen lukutaito Moduuli 6 TVT:n epäasialliseen käyttöön puuttuminen (virtuaalinen kiusaaminen ja seksuaalissävytteinen viestittely) Moduulien 7 ja 8 osat, jotka liittyvät digitaalisen turvallisuuden opetussuunnitelmaan **Vaihtoehtoisesti kolmipäiväinen kurssi opettajille** Moduuli 1 Digitaalinen turvallisuus koulussa ja luokassa Moduuli 2 Digitaalista turvallisuutta nuorille ja opettajille Moduuli 3 Digitaalinen turvallisuus: digikansalaisuus Moduuli 5 Digitaalinen turvallisuus: digitaalinen lukutaito Moduuli 6 TVT:n epäasialliseen käyttöön puuttuminen (virtuaalinen kiusaaminen ja seksuaalissävytteinen viestittely) Moduuli 7 Käytännön lähestymistapoja digitaaliseen turvallisuuteen oppitunneilla **Vaihtoehtoisesti kaksipäiväinen kurssi opettajille** Moduuli 1 Digitaalinen turvallisuus koulussa ja luokassa Moduuli 4 Digitaalinen turvallisuus: henkilökohtainen turvallisuus ja hyvinvointi Moduuli 5 Digitaalinen turvallisuus: digitaalinen lukutaito Moduuli 7 Käytännön lähestymistapoja digitaaliseen turvallisuuteen oppitunneilla **tai** Moduuli 1 Digitaalinen turvallisuus koulussa ja luokassa Moduuli 3 Digitaalinen turvallisuus: digikansalaisuus Moduuli 5 Digitaalinen turvallisuus: digitaalinen lukutaito Moduuli 6 TVT:n epäasialliseen käyttöön puuttuminen (virtuaalinen kiusaaminen ja seksuaalissävytteinen viestittely) **tai** Moduuli 5 Digitaalinen turvallisuus: digitaalinen lukutaito Moduuli 6 TVT:n epäasialliseen käyttöön puuttuminen (virtuaalinen kiusaaminen ja seksuaalissävytteinen viestittely)

	Moduuli 7 Käytännön lähestymistapoja digitaaliseen turvallisuuteen oppitunneilla Moduuli 8 Digitaalinen turvallisuus koulun opetussuunnitelmassa **Vaihtoehtoisesti kaksipäiväinen kurssi koulujen opinto-ohjaajille ja oppilaanohjaajille** Moduuli 1 Digitaalinen turvallisuus koulussa ja luokassa Moduuli 2 Digitaalista turvallisuutta nuorille ja opettajille Moduuli 3 Digitaalinen turvallisuus: digikansalaisuus Moduuli 6 TVT:n epäasialliseen käyttöön puuttuminen (virtuaalinen kiusaaminen ja seksuaalissävytteinen viestittely) **Vaihtoehtoisesti kaksipäiväinen koulutus rehtoreille ja tieto- ja viestintätekniikasta vastaaville opettajille** Moduuli 1 Digitaalinen turvallisuus koulussa ja luokassa Moduuli 2 Digitaalista turvallisuutta nuorille ja opettajille Moduuli 9 Koko koulun digitaalisen turvallisuuden ohjelma Moduuli 10 Toimintasuunnitelma digitaalisen turvallisuuden ohjelman parantamiseksi **tai** Moduuli 1 Digitaalinen turvallisuus koulussa ja luokassa Moduuli 6 TVT:n epäasialliseen käyttöön puuttuminen (virtuaalinen kiusaaminen ja seksuaalissävytteinen viestittely) Moduuli 9 Koko koulun digitaalisen turvallisuuden ohjelma Moduuli 10 Toimintasuunnitelma digitaalisen turvallisuuden ohjelman parantamiseksi **Vaihtoehtoisesti yksipäiväinen kurssi rehtoreille ja tieto- ja viestintätekniikasta vastaaville opettajille** Moduuli 9 Koko koulun digitaalisen turvallisuuden ohjelma Moduuli 10 Toimintasuunnitelma digitaalisen turvallisuuden ohjelman parantamiseksi
Osallistumistodistus	Osallistujien tulisi saada osallistumistodistus kurssin viimeisenä päivänä. Kurssin virallinen hyväksilukeminen vaihtelee maittain.

Digitaalinen turvallisuus – ohjelmarunko

Moduuli	Nimi	Kesto Noin
Päivä 1	**Digitaalinen turvallisuus 2000-luvulla**	
Mod. 1	**Digitaalinen turvallisuus koulussa ja luokassa**	**2,5 h**
	Tervetulosanat ja johdanto Koulujen parhaiden käytäntöjen tarkastelu Digitaalisen turvallisuuden määrittely EU:n kouluille ja opettajille suunnattujen digitaalisen turvallisuuden materiaalien tutkiminen ja tallentaminen kirjanmerkkeihin	
Mod. 2	**Digitaalista turvallisuutta nuorille ja opettajille**	**3 h**
	Digitaalinen lukutaito ja digikansalaisuus: Mitä ne tarkoittavat digitaalisen turvallisuuden kannalta? Riskit ja mahdollisuudet Internetin turvallisempi käyttö Opittavat asiat ja pohdintaa	
Päivä 2	**Digitaalinen turvallisuus opetuksessa ja oppimisessa**	
Mod. 3	**Digitaalisen turvallisuuden taidot: digikansalaisuus**	**3 h**
	Digitaalinen turvallisuus ja sosiaalisen median työkalut Mobiililaitteiden vastuullisen käytön opettaminen Pedagogisten tietolähteiden ja materiaalien kerääminen Materiaalien esittely – Teachmeet-tyyliin	
Mod. 4	**Digitaalisen turvallisuuden johtaminen: henkilökohtainen turvallisuus ja hyvinvointi**	**3 h**
	Digitaalisen turvallisuuden kysymykset, jotka liittyvät verkkomaineeseen ja yksityisyyteen Käytännön ryhmätyö – oppitunnin rakentaminen Ideoiden jakaminen oppitunteja varten – Teachmeet-menetelmä Opittavat asiat ja pohdintaa	
Päivä 3	**Kriittinen ajattelu ja pohdinta**	
Mod. 5	**Digitaalinen turvallisuus ja asianmukainen käyttö: digitaalinen lukutaito**	**3 h**
	Kriittisen ajattelun ja informaatiolukutaidon opettaminen Kuinka luon luokkaympäristön, jossa digitaalinen turvallisuus on otettu huomioon? Digitaalisten lukutaitojen opettaminen Opetus- ja oppimistapojen ja materiaalien jakaminen: Teachmeet-menetelmä	
Mod. 6	**TVT:n epäasialliseen käyttöön puuttuminen: virtuaalinen kiusaaminen ja seksuaalissävytteinen viestittely**	**3 h**
	Mitä on virtuaalinen kiusaaminen? Koko koulun tapa puuttua virtuaaliseen kiusaamiseen Seksuaalissävytteinen viestittely – ongelmat ja haasteet Seksuaalissävytteinen viestittely – ehkäisevät toimet ja tukeminen Oppimisen pohdintaa	
Päivä 4	**Käytännön vinkkejä toteutettavaksi**	
Mod. 7	**Käytännön lähestymistapoja digitaaliseen turvallisuuteen oppitunneilla**	**3 h**
	Digitaalisten työkalujen turvallinen käyttö opetuksessa ja oppimisessa Opetussuunnitelmaan perustuvan tuntisuunnitelman tekeminen	

	Käsitelläänkö oppitunneilla keskeisiä asioita? Koko koulun digitaalisen turvallisuuden opetussuunnitelman luonnostelu	
Mod. 8	**Digitaalinen turvallisuus koulun opetussuunnitelmassa ja sen ulkopuolella**	3 h
	Oppilaat, Internet-turvallisuuden teemapäivä (Safer Internet Day) ja vertaismentorointi Vanhempien osallistaminen Asteittain etenevä koko koulun digitaalisen turvallisuuden opetussuunnitelma Digitaalisen turvallisuuden vieminen omaan kouluun Oppimispäiväkirja	
Päivä 5	**Digitaalisen turvallisuuden ohjelma omalle koululle**	
Mod. 9	**Koko koulun digitaalisen turvallisuuden ohjelma**	**3 h**
	Digitaalisen turvallisuuden ohjelman suunnittelu omalle koululle EU:n eSafety Label -hanke Digitaaliseen turvallisuuteen liittyvien ongelmatapausten hoitaminen omassa koulussa Olemmeko valmiita omien laitteiden (BYOT) tai henkilökohtaiseen käyttöön annettujen laitteiden käyttöön (1:1)? Digitaalisen turvallisuuden itsearviointi omassa koulussa	
Mod. 10	**Digitaalisen turvallisuuden toimintasuunnitelman luominen**	**3 h**
	Esimerkki eSafety Label -toimintasuunnitelmasta eSafety Label -toimintasuunnitelman käyttäminen oman koulun digitaalisen turvallisuuden ohjelman kehittämisessä Keskustelua toimintasuunnitelmasta jatkossa? Johtopäätökset ja arviointi Todistustenjakotilaisuus ja kurssin päätös	

Digitaalisen turvallisuuden kurssin runko

	Päivä 1	Päivä 2	Päivä 3	Päivä 4	Päivä 5	
Minä ja kouluni	Digitaalinen turvallisuus 2000-luvulla	Digitaalinen turvallisuus opetuksessa ja oppimisessa	Kriittinen ajattelu ja pohdinta	Käytännön vinkkejä toteutettavaksi	Digitaalisen turvallisuuden ohjelma omalle koululle	Minä ja kouluni
	Digitaalinen turvallisuus koulussa ja luokassa (moduuli 1)	Digitaalisen turvallisuuden taidot: digikansalaisuus (moduuli 3)	Digitaalinen turvallisuus ja asianmukainen käyttö: digitaalinen lukutaito (moduuli 5)	Käytännön lähestymistapoja digitaaliseen turvallisuuteen oppitunneilla (moduuli 7)	Koko koulun digitaalisen turvallisuuden ohjelma (moduuli 9)	
	Keskustelua: - kysymykset ja ongelmat - ratkaisut	Teoria ja käytäntö	Taidot ja työkalut	Pohdinta ja kriittinen ajattelu	Oman koulun digitaalisen turvallisuuden ohjelma	
	Digitaalista turvallisuutta nuorille ja opettajille (moduuli 2)	Digitaalisen turvallisuuden johtaminen: henkilökohtainen turvallisuus ja hyvinvointi (moduuli 4)	TVT:n epäasialliseen käyttöön puuttuminen: virtuaalinen kiusaaminen ja seksuaalissävytteinen viestittely (moduuli 6)	Digitaalinen turvallisuus koulun opetussuunnitelmassa ja sen ulkopuolella (moduuli 8)	Digitaalisen turvallisuuden toimintasuunnitelman luominen (moduuli 10)	

Vaatimukset osanottajille ennen ja jälkeen kurssin

Vaatimukset ennen kurssia (viisipäiväinen kurssi)	Osallistujilla tulee olla perustaidot tieto- ja viestintätekniikan käytössä sekä kiinnostus digitaalisen teknologian ja Internetin käyttöön opetuksessa ja oppimisessa. Osallistujia pyydetään ottamaan mukaan oma kannettava tietokoneensa sekä tallennusväline, kuten USB-muistitikku. Lisäksi osallistujilla tulee olla käytössä tilapäinen sähköpostiosoite ja heidän tulee tehdä seuraavat ennakkotehtävät ennen kurssia: Haastattele kahta kollegaa koulullasi ja mieti sen jälkeen kolme myönteistä tekniikan käyttötapaa sekä kolme haastavampaa tai ongelmallisempaa tekniikan käyttöön liittyvää osa-aluetta, joista koulullasi on kokemusta. Harjoitus moduulia 1 varten: **kerro digitaaliseen turvallisuuteen liittyvistä positiivisista kokemuksista ja haasteista *täällä*** [Paikalliset kouluttajat lisäävät linkin lyhyeen verkkokyselyyn sanan 'täällä' kohdalle. Kyselyn tekemiseen voi käyttää ilmaisia työkaluja, kuten surveymonkey.com] Luettele esimerkkejä erilaisista digitaaliseen turvallisuuteen liittyvistä kysymyksistä, joita oppilaat ja opettajat saattavat kohdata käyttäessään Internetiä, digitaalisia työkaluja, mobiililaitteita ja sosiaalista mediaa sekä koulussa että sen ulkopuolella. Kuinka nämä digitaaliseen turvallisuuteen liittyvät kysymykset on otettu huomioon koulusi tietojärjestelmien käyttöehdoissa tai digitaalisen turvallisuuden toimintaohjeissa? Tehtävä moduulia 2 varten: ota mukaasi kopio koulusi tietojärjestelmien käyttöehdoista tai linkki niihin. Käsitelläänkö koulusi toimintaohjeissa kiusaamista ja virtuaalista kiusaamista? Missä toimintaohjeissa näitä ongelmia käsitellään? Kuvaa, kuinka koulussasi käsitellään virtuaaliset kiusaamistapaukset. Onko koululla oppitunteja tai opetusohjelmaa, joka käsittelee virtuaalista kiusaamista? Kuka pitää oppitunnit tai vetää opetusohjelmaa? Millaista ohjausta ja tukea on saatavilla paikallisella, alueellisella ja kansallisella tasolla? Millaisia materiaaleja on käytetty onnistuneesti? Harjoitus moduulia 6 varten: luo digitaalinen luettelo kaikista oppitunneista ja hyvistä käytännöistä, joiden avulla koulussasi on puututtu onnistuneesti virtuaaliseen kiusaamiseen. Tuo luettelo mukanasi kurssille. **Huom.: Tämä harjoitus on tarkoitettu ainoastaan rehtoreille tai tieto- ja viestintätekniikasta vastaaville opettajille, jotka osallistuvat lyhyelle, moduuleista 9 ja 10 koostuvalle kurssille.** Lue asiakirja eS 10 – Yhteenveto tutkimustuloksista. Se tarjoaa yleiskatsauksen ajankohtaisista digitaaliseen turvallisuuteen liittyvistä kysymyksistä. Mitä näistä kysymyksistä ja ongelmista on käsitelty omassa koulussasi? Kuinka näitä kysymyksiä voi hyödyntää koko koulun digitaalisen turvallisuuden ohjelman hahmottelussa?

	a. Kuinka digitaaliseen turvallisuuteen liittyvät kysymykset otetaan huomioon luokkaympäristössä opetuksen ja oppimisen yhteydessä? Onko koulussasi asteittain etenevä koko koulun digitaalisen turvallisuuden opetussuunnitelma? b. Mitä digitaaliseen turvallisuuteen liittyviä toimintaohjeita koulussasi on? Milloin ne on viimeksi tarkistettu ja päivitetty? Ovatko koulusi digilaitteiden käyttöehdot ja toimintaohjeet saatavilla sellaisella kielellä ja muodossa, että oppilaiden on helppo ymmärtää ne? c. Tarjotaanko henkilökunnalle koulun sisäistä koulutusta ja työpajoja, jotka käsittelevät koulun tieto- ja viestintätekniikan turvallista ja asianmukaista opetus- ja oppimiskäyttöä?
Kurssin jälkeiset jatkotoimenpiteet	Kurssin aikana osallistujia kehotetaan tutustumaan asiantuntijatietoon ja aineistoihin, jotka ovat käytettävissä Insafe-verkoston kautta www.saferinternet.org. Heidän tulisi tilata SaferInternetDay- ja Insafe-uutiskirjeet. Kurssin jälkeen osallistujia tulisi kannustaa tekemään omat digitaalisen turvallisuuden toimintasuunnitelmansa. Vapaaehtoisessa jatkowebinaarissa käsitellään sitä, kuinka osallistujat ja heidän koulunsa toteuttavat digitaalisen turvallisuuden käytäntöjä ja digitaalista turvallisuutta edistävää opetussuunnitelmaa.
Koulutukseen vaadittavat kurssimateriaalit	Paikallisten kouluttajien tulisi perustaa ryhmälle verkko-oppimisympäristö (esim. Moodle, Schoology), jossa voidaan jakaa kurssin sisältöä tukevia aineistoja ja joka sisältää keskustelufoorumin ja paikan, jossa osallistujat voivat pohtia opittuja asioita. Oppimisalusta rohkaisee osallistujia aktiiviseen, osallistavaan, sosiaaliseen oppimiseen ja omien materiaalien jakamiseen. **Osallistujille jaettava materiaali:** The Web We Want (Insafe ja EUN) Using Mobile Phone in School (Insafe ja EUN) – jos saatavilla Insafe DigiPacks 2010–2012 Monisteet: eS 1.1 eS 2.2a eS 3.2a eS 5.1a eS 5.1b eS 5.1c eS 5.2a eS 7.2 eS 7.4 eS 8.5a eS 8.5b eS 9.3a eS.9.3b eS 10.1 eS 10.2b Kun rehtoreille ja tieto- ja viestintätekniikasta vastaaville opettajille pidetään moduulit 9 ja 10 kattava kurssi, heille lähetetään seuraava asiakirja ennen kurssia: 10.1 – Yhteenveto tutkimustuloksista
Kouluttajan tehtävät ennen kurssia	• Virtuaalisen oppimisympäristön ja Twitter-tilin perustaminen sekä lyhyen SurveyMonkey-tyyppisen kyselyn tekeminen ennakkotehtävää 1 varten. • Kouluttaja liittyy eSafety Label -sivustolle ja tekee arviointikyselyn (Assessment

	Quiz) oppiakseen ymmärtämään prosessia ja voidakseen esitellä sitä kurssin aikana.

Kouluttajan käsikirja ja tukimateriaalit

Kurssi:

Digitaalinen turvallisuus: TURVALLISEMPI KOULU JA LUOKKAYMPÄRISTÖ

Moduuli 1: Digitaalinen turvallisuus koulussa ja luokassa

(eS 1.0)

eS 1.0: Digitaalinen turvallisuus koulussa ja luokassa

CPDLab-kurssi	Digitaalinen turvallisuus: turvallisempi koulu ja luokkaympäristö
Moduulin numero	**eS 1.0**
Moduulin nimi	**Digitaalinen turvallisuus koulussa ja luokassa**
Vaatimukset moduulin suorittamiseen	• Osallistujilla tulee olla perustaidot tieto- ja viestintätekniikan käytössä ja kiinnostus digitaalisen teknologian ja Internetin käyttöön opetuksessa ja oppimisessa. • Jokainen osallistuja tarvitsee tilapäisen sähköpostiosoitteen, jonka avulla luodaan tili sosiaaliseen kirjanmerkkipalveluun. • Osallistujien tulee suorittaa seuraava **ennakkotehtävä** ennen kurssia: Haastattele kahta kollegaasi koululla ja mieti kolme myönteistä teknologian käyttötapaa ja kolme haastavampaa tai ongelmallisempaa osa-aluetta, joita koulullasi on kohdattu teknologian käytössä. Harjoitus moduulia 1 varten:
Kesto	2,5 h
Kurssipaikka ja moduulin rakenne	• Tämä moduuli järjestetään lähiopetuksena. • Osallistujia kehotetaan ottamaan mukaan oma kannettava tietokoneensa, sillä moduulin aikana kokeillaan opetettavia asioita käytännössä. • Lisäksi moduuliin kuuluu tehtäviä, keskustelua, ryhmätöitä ja pohdintaa. • Osallistujia rohkaistaan jatkuvasti etsimään ja valikoimaan materiaalia ja linkkejä heidän omalla kielellään.
Tarvittavat tilat ja tilajärjestelyt	• Kouluttaja tarvitsee käyttöönsä kosketustaulun, tietokoneen ja langattoman verkon. • Jokainen osallistuja tarvitsee tietokoneen, jossa on Internet-yhteys. • Tiloissa tulisi olla tarpeeksi virtapistokkeita kannettaville tietokoneille. • Lisäksi osallistujat tarvitsevat tiloja 3–5 hengen pienryhmätyöskentelyyn.

Moduulin yleiskuvaus	• Tervetulosanat ja osallistujien esittely • Tunnelmaa rentouttamaan - Ihmisbingo digikansalaisille • Kurssin, tilojen ja työkalujen esittely • Koulujen parhaiden käytäntöjen tarkastelua • Opettajan rooli digitaalisessa turvallisuudessa (paritehtävä, osallistujien ennakkotehtävänä tekemä tehtävä 1 toimii myös pohjana jatkokeskusteluun.) • Ryhmätyö: SWOT-analyysi hyödyntämällä osallistujien kokemuksia, joita kar-

	toitettiin ennakkotehtävän 1 yhteydessä.
Moduulin tavoitteet	• toivottaa osallistujat tervetulleeksi ja esitellä heille kurssin ohjelma • kehittää strategioita Internetin ja digiteknologian turvalliseen käyttöön opetuksessa ja oppimisessa • tarkastella, kuinka koulut voivat luoda turvallisia oppimisympäristöjä ja suojella oppilaita sekä sisällyttää digitaalisen turvallisuuden koulun opetussuunnitelmaan ja kaikkeen koulun toimintaan • ymmärtää keskeiset digitaaliseen turvallisuuteen liittyvät riskit ja se, että riskeihin on puututtava ennakoivasti koko koulun asteittain etenevän digitaalisen turvallisuuden suunnitelman kautta • ymmärtää koulujen digitaalisen turvallisuuden toimintaohjeiden tarpeellisuus; ohjeistuksen tulee olla helposti ymmärrettävissä ja kaikkien saatavilla ja sitä tulisi arvioida ja päivittää säännöllisesti • ymmärtää koulun digitaalisen turvallisuuden ohjelman kolme olennaista osatekijää.
Taitojen ja osaamisen karttuminen moduulissa	Osallistujat oppivat • aloittamaan sosiaalisen median työkalun käytön ja käyttämään työkalua • tunnistamaan keskeiset digitaalisen turvallisuuden kysymykset, jotka vaikuttavat opettajiin ja oppilaisiin • miettimään erilaisia opetusmateriaaleja ja lähestymistapoja digitaalisen turvallisuuden opettamiseen • tekemään yhteistyötä ja jakamaan kokemuksia muiden opettajien kanssa verkossa • miettimään erilaisia opetus- ja oppimisstrategioita • harjoittelemaan uusia taitoja käyttämällä oppimisessa digitaalisia työkaluja, kuten bloggaamista.
Tarvittavat materiaalit ja välineet	• Monisteet: eS 1.1 • Kouluttajalle tietokone, jossa on Internet-yhteys, ja dataprojektori sekä kosketustaulu. • Kannettavat tietokoneet osallistujille ja pääsy langattomaan verkkoon. • Salasanat kurssisisältöalueelle (Course Content Online Area) ja oppimispäiväkirjaan ja keskustelualueelle (Learning Reflection Area). • Ennen kurssin alkua kouluttaja luo ryhmälle verkko-oppimisympäristön käyttämällä oppimisalustaa ja jakaa tunnukset moduulin 1 aikana.
Vaatimukset kouluttajalle	• Kouluttajalla tulee olla syvällinen ja monipuolinen tietämys digitaalisesta lukutaidosta, digitaaliseen turvallisuuteen liittyvistä kysymyksistä ja digitaalisen turvallisuuden opetussuunnitelmista. • Kouluttajan tulee tuntea EU:n politiikka, joka tähtää Internetin parantamiseen lasten ja nuorten näkökulmasta, Insafen materiaalit ja palvelut sekä paikallisen Safer Internet Centren materiaalit ja kansainvälinen digitaalisen turvallisuuden opetussuunnitelma. • Kouluttajan tulee tutustua kurssin verkkoalueeseen ja kaikkiin kurssin tuki-

	materiaaleihin, jotka on listattu jokaisen moduulin lopussa. Jokainen materiaali on listattu kurssin, moduulin ja tehtävän mukaan, esim. eS 1.1 "Ihmisbingo digikansalaisille" • Kouluttajan tulee käyttää sosiaalista kirjanmerkkipalvelua (esim. www.delicious.com tai Diigo www.diigo.com), jonne tallennetaan digitaaliseen turvallisuuteen liittyviä linkkejä ja materiaaleja. • Kouluttajan tulee myös kannustaa osallistujia luomaan oma käyttäjätili, jonka avulla he voivat hallita kurssilla jaettuja verkko-osoitteita ja materiaaleja.
Lähdeaineistoja ja materiaaleja kouluttajille	**Insafe** www.saferInternet.org Osittain Euroopan unionin rahoittama Insafe on eurooppalainen Safer Internet Centre -verkosto, joka edistää turvallista ja vastuullista Internetin ja mobiililaitteiden käyttöä nuorten keskuudessa. Se tarjoaa laajan valikoiman materiaaleja ja tietolähteitä useilla eri kielillä. Jokaisella jäsenmaalla on oma **Safer Internet Awareness Centrensä.** On mahdollista hyödyntää myös muiden maiden (esimerkiksi englannin- tai ruotsinkielisiä) Safer Internet Awareness Centre-aineistoja. **Safer Internet Day** (SID) www.saferInternetday.org Helmikuun toisena tiistaina vietetään kouluissa vuosittain kansainvälistä Internet-turvallisuuden teemapäivää (Safer Internet Day). EU:n hanke tarjoaa materiaaleja, oppituntisuunnitelmia ja teemapaketteja opettajille ja kouluille. **Euroopan komissio** "Eurooppalainen strategia Internetin parantamiseksi lasten näkökulmasta", saatavana useilla eri kielillä: http://ec.europa.eu/information_society/activities/sip/policy/index_en.htm **Teach today** www.teachtoday.eu/ Teachtoday-sivusto tarjoaa opettajille, rehtoreille ja muille koulun työntekijöille tietoa ja neuvoja uuden tekniikan myönteiseen, vastuulliseen ja turvalliseen hyödyntämiseen. Sivustolla olevien tapausesimerkkien avulla kouluttajat voivat herättää keskustelua osallistujien kohtaamista todellisista ongelmista kouluissa. www.teachtoday.eu/en/Case-studies.aspx EUN:in raportti "Teaching with Technology in 2011" käsittelee koulujen ja luokkaympäristön digitaaliseen turvallisuuteen liittyviä opettajien tarpeita ja toiveita ja tarjoaa kouluttajille yleiskatsauksen aiheeseen. www.teachtoday.eu/sitecore/shell/Applications/~/media/Files/United%20Kingdom/pdf/Teaching%20with%20technology%202011%20survey%20report%202011.ashx?db=master

	EU Kids Online www.eukidsonline.net Projektin tavoitteena on lisätä ja koordinoida lasten verkon käyttöä ja toimintaa sekä riskejä ja turvallisuutta käsittelevää tutkimusta. Sitä on kuvattu teoreettiselta pohjaltaan vankimmaksi ja metodologisesti kehittyneimmäksi digitaalisen ympäristön riskejä ja mahdollisuuksia tarkastelevaksi tutkimukseksi. Koko raportti: www2.lse.ac.uk/media@lse/research/EUKidsOnline/EUKidsII%20(2009-11)/EUKidsOnlineIIReports/D4FullFindings.pdf Yhteenveto: www2.lse.ac.uk/media@lse/research/EUKidsOnline/EU%20Kids%20II%20(2009-11)/EUKidsOnlineIIReports/EUKidsOnlineII,summary,v2.pdf **Byron Review –raportti** www.dcsf.gov.uk/byronreview "Safer Children in a Digital World" (Digitaalinen maailma turvallisemmaksi lapsille) **Digitaalinen osaaminen ja digitaalinen lukutaito** http://linked.eun.org/web/guest/policyMaker Osittain Euroopan komission rahoittama projekti, joka tarkastelee tieto- ja viestintätekniikkaa hyödyntävän, innovatiivisen opetuksen ja oppimisen tutkimusta, politiikkaa ja käytäntöjä. **Connected Learning** http://clrn.dmlhub.net/resources/videos Monitieteinen tutkimusverkosto, tarkastelukohteena nykyisen muuttuvan mediaympäristön tarjoamat oppimismahdollisuudet ja toisaalta sen aiheuttamat riskit. **Pew Internet & American Life -projekti** www.pewinternet.org Ajantasaista tietoa digitaaliseen teknologiaan liittyvistä kysymyksistä ***UNESCO* Pedagogies of Media and Information Literacies -käsikirja** http://iite.unesco.org/pics/publications/en/files/3214705.pdf. **Digizen** www.digizen.org Digizen-sivusto tarjoaa tietoa opettajille, vanhemmille, huoltajille ja nuorille. Sen tarkoituksena on rohkaista teknologian käyttäjiä olemaan vastuullisia digikansalaisia. Sivustolla jaetaan neuvoja ja materiaaleja, jotka käsittelevät esimerkiksi verkkoyhteisöjä ja virtuaalista kiusaamista ja sitä, miten ne liittyvät ja vaikuttavat ihmisten käyttäytymiseen ja kokemuksiin verkossa.
Arviointi-vaihtoehdot	• Osallistujat keskustelevat kokemuksistaan ja niiden yhtäläisyyksistä ja eroista ennakkotehtävän 1 perusteella. • Osallistujat luovat tilin sosiaaliseen kirjanmerkkipalveluun ja jakavat linkkinsä julkisesti (valitsemalla asetukseksi 'Public'). • Osallistujat kirjoittavat ensimmäisen merkinnän keskustelualueelle tai blogiin.

Moduulin jälkeiset jatkotoimenpiteet	Ei ole.
Vaihtoehtoiset tavat toteuttaa moduuli	Ei vaihtoehtoisia toteuttamistapoja.
Toteuttamisvaihtoehdot kansallisella/paikallisella tasolla	Tämä moduuli voidaan toteuttaa kansallisella/paikallisella tasolla. Se käsittelee digitaalisen turvallisuuden peruskäsitteitä opettajien ja koulujen näkökulmasta, sekä sitä, miksi digitaalinen lukutaito vaatii digitaalisen turvallisuuden tuntemusta ja taitoja. Osallistujat tutustuvat toisiinsa, jakavat kokemuksia omista kouluistaan ja pohtivat, miksi digitaalinen turvallisuus tulisi sisällyttää opetussuunnitelmaan ja kaikkeen koulun toimintaan. Moduulin tulisi kuulua jokaiseen moduuliyhdistelmään.
Tehtävä 1.1	**Tervetulosanat ja esittelyt**
Kesto	15 min
Tavoitteet	• tutustutaan osallistujiin ja heidän digitaaliseen elämäänsä • kartoitetaan osallistujien odotukset.
Kuvaus	Epämuodollinen tilaisuus tutustua muihin osallistujiin ja jakaa käsityksiä siitä, miten digitaaliseen mediaan liittyvät kysymykset vaikuttavat osallistujien omaan ja oppilaiden arkeen. • Tunnelman keventäminen ja osallistujien esittely toisilleen Kouluttaja jakaa jokaiselle osallistujalle ihmisbingo-taulukon eS 1.1 Ihmis bingo digikansalaisille. Ensimmäisenä tarvittavan määrän nimiä ja syitä kokoon saava osallistuja huutaa 'Bingo!' ja hänet julistetaan voittajaksi. Kouluttaja antaa pienen palkinnon (esim. kynä, suklaata) ja alustaa sitten lyhyen keskustelun siitä, kuinka elämästä on tullut digitaalista ja kuinka jatkuva verkossa oleminen vaikuttaa oppilaiden arkeen. Tämän tulisi toimia johdantona tehtävään 1.2. *TAI* • Tunnelman keventäminen kirjaamalla osallistujien odotukset Post-it-lapuille. Osallistujat jaetaan neljän hengen ryhmiin. Jokaisella osallistujalla on noin minuutti aikaa kirjoittaa kurssia koskevat odotuksensa post-it-lapulle. Jokainen pienryhmä kokoaa vastauksensa ja kertoo sitten oman ryhmänsä odotukset muille ryhmille. Kouluttaja kokoaa odotukset.
Tehtävä 1.2	**Yleiskatsaus kurssin sisältöön ja kurssijärjestelyihin**
Kesto	15 min
Tavoitteet	Tutustua kurssin sisältöön ja kurssijärjestelyihin.

Kuvaus	Kouluttaja kuvaa tiiviisti kurssin sisällöt (eS 1.2 Digitaalisen turvallisuuden kurssin yleiskatsaus ppt) • **@ Diassa 3** Kuvataan kurssijärjestelyt (esim. langattoman verkon tiedot, lounas jne.). Esitellään kurssin verkko-oppimisympäristö ja pääsy tukimateriaaleihin. Kouluttaja varmistaa, että kaikki osallistujat pääsevät kirjautumaan kurssijärjestelmään ja käyttämään tukimateriaaleja. Kouluttaja sopii osallistujien kanssa, kuinka keskeiset opittavat asiat ja pohdinnat tallennetaan jokaisen päivän päätteeksi. Tässä voi käyttää esimerkiksi oppimisalustaa tai Wordpress-blogia, Moodlea, Etherpadia, Ning-palvelua tai Google+-palvelua. Huom.: Jos kurssi pidetään EUN:in tiloissa, tässä välissä voidaan käydä tutustumassa Future Classroom Lab -tiloihin.
Tehtävä 1.3	**Digitaalinen turvallisuus koulussa ja luokassa**
Kesto	50 min
Tavoitteet	• pohtia parhaita käytäntöjä digitaalisen turvallisuuden toteuttamiseksi kouluissa • vertailla digitaaliseen turvallisuuteen liittyviä kysymyksiä eri Euroopan maiden opettajien näkökulmasta • jakaa kollegojen ja nuorten kokemuksia vaikeista tai haastavista digitaaliseen turvallisuuteen liittyvistä tilanteista sekä saada yleiskatsaus eri koulujen parhaista käytännöistä.
Kuvaus	Kouluttaja aloittaa PowerPoint-esityksen eS 1.3 Digitaalinen turvallisuus koulussa ja luokassa pptx. Dioissa on mukana esittäjän muistiinpanot. • **@ Dia 5** Kouluttaja kysyy ryhmältä heidän koulujensa digitaalisen turvallisuuden käytäntöjä ja kirjoittaa ne kosketustaululle. Osallistujat mainitsevat todennäköisesti seuraavia aihepiirejä: tietojärjestelmien käyttöehdot, tieto- ja viestintätekniikan käytön ohjeistus, mobiililaiteohjeistus, omien laitteiden käyttöön liittyvä ohjeistus, sosiaalisen median ohjeistus. Jos keskustelu ei etene, kouluttaja voi johdatella osallistujia esimerkiksi seuraavilla kysymyksillä: Tuntevatko kaikki säännöt ja ohjeistukset? Tuntevatko koulun uudet opettajat ne? Tietävätkö oppilaat niistä? Ja ymmärtävät ne? Onko osallistujilla ehdotuksia, miten yksinkertaistaa tai virtaviivaistaa sääntöjä ja ohjeistuksia ja tehdä niistä tehokkaampia? • **@ Dia 7** Kouluttaja näyttää 2:28 minuuttia kestävän videon http://www.youtube.com/watch?v=F7pYHN9iC9I&sns=em Sen jälkeen lyhyt keskustelu. • **@ Dia 8** Kouluttaja avaa kosketustaululla sivuston www.padlet.com ja luo ryhmälle seinän. Kouluttaja antaa seinälle nimen ja jakaa seinän ryhmän kanssa. Hän

	pyytää osallistujia miettimään pareittain ehdotuksia digitaalisen turvallisuuden käytännöiksi, joita opettajat voivat esitellä päivittäin luokassa. Jokainen pari jakaa ehdotuksensa seinällä. Sen jälkeen kouluttaja pyytää ehdotuksia ryhmäläisiltä käytäntöjen jaottele miseksi aihepiireittäin, joita voivat olla esim. Digitaalinen lukutaito, Henkilö kohtainen turvallisuus ja hyvinvointi sekä Digikansalaisuus. Todennäköisiä ehdotuksia ovat esimerkiksi tiedon ja kuvien turvallinen etsiminen, henkilö kohtaisten tietojen suojaaminen, valokuvien ja tietojen tietosuoja, tekijänoikeuslain noudattaminen, lähteiden merkitseminen ja plagioinnin välttämi nen, turvallisuusasetusten käyttäminen, selainten ja laitteiden päivitykset, virustorjunnan käyttäminen, kunnioittava ja asianmukainen viestintä. Kouluttaja kysyy ryhmältä, minkä edellä mainitun kolmen otsikon alle ne heidän mielestään kuuluvat. Ryhmittely auttaa osallistujia hahmottelemaan digitaalisen turvallisuuden määritelmää seuraavan tehtävän aikana. • **@ Dia 9** Muodostetaan neljä uutta ryhmää (kussakin 3–5 jäsentä, jotka eivät ole vielä työskennelleet yhdessä) tekee SWOT-analyysin ennakkotehtävän 1 pohjalta. He voivat esittää SWOT-analyysinsa muulle ryhmälle haluamallaan tavalla (fläppitaulu, kosketustaulu...) **Ryhmä 1:** Vahvuuksien analysointi – oppilaiden Internetin ja digitaalisen median käyttö. **Ryhmä 2:** Heikkouksien analysointi – oppilaiden Internetin ja digitaalisen median käyttö. **Ryhmä 3:** Mahdollisuuksien analysointi – oppilaiden Internetin ja digitaalisen median käyttö **Ryhmä 4:** Uhkien analysointi – oppilaiden Internetin ja digitaalisen median käyttö. Palautetta koko ryhmälle, kouluttaja kirjaa pääkohdat kosketustaululle. Moduulin tehtävä 1.3 loppuu. Kahvitauko.
	Kahvitauko 15 min
Tehtävä 1.4	**Digitaalisen turvallisuuden määritelmä?**
Kesto	20 min
Tavoitteet	• jakaa palautetta ryhmätyönä tehtyjen SWOT-analyysien perusteella. • saada SWOT-analyysien perusteella yleiskuva osallistujien tarpeista ja nykyisestä osaamisesta ja taidoista digitaalisen turvallisuuden alalla, sekä heidän kurssille asettamistaan odotuksista • jakaa osallistujien kesken kokemuksia ennakkotehtävän 1 pohjalta • luoda yhteinen digitaalisen turvallisuuden määritelmä.
Kuvaus	Ryhmä keskustelee SWOT-analyysistä, joka näkyy edelleen interaktiivisella valkotaululla. Kouluttaja ja osallistujat kokoavat yhdessä luettelon digitaalisen turvallisuuden tärkeimmistä osatekijöistä ja näkökulmista. Jokainen pienryhmä avaa sitten yhteiseen kirjoittamiseen tarkoitetun verkkomuistion (esim. Etherpad:

	http://etherpad.opensourcebridge.org), johon he kirjaavat digitaalisen turvallisuuden määritelmän yhdellä lauseella. Jokainen ryhmä lähettää muistion linkin kouluttajalle sähköpostilla. Lounaan aikana kouluttaja siirtää määritelmät diaan 9 - eS 2.1 Digitaalinen turvallisuus ja digitaalinen lukutaito **Tiedoksi kouluttajalle:** Digitaalinen turvallisuus koulutuksessa on yhdistelmä henkilökohtaista turvallisuutta, digitaalista lukutaitoa ja digikansalaisuutta. Ymmärrys tästä kehittyy kurssin myötä. Älä anna yllä olevaa määritelmää ryhmälle vaan anna heidän työstää omia määritelmiään.
Tehtävä 1.5	**EU:n opettajille ja kouluille tarkoitettujen digitaalisen turvallisuuden tietolähteiden ja materiaalien etsiminen ja kirjanmerkkien lisääminen**
Kesto	45 min
Tavoitteet	• Tutkia Insafe-verkoston opettajille ja kouluille suunnattuja materiaaleja ja työkaluja. • Kehittää digitaalista osaamista käyttämällä opettajille ja oppilaille tarkoitettua sosiaalista kirjanmerkkipalvelua. • Tunnistaa digitaalisen työnkalun rajoitukset ja miettiä, kuinka siihen liittyviä riskejä voi hallita.
Kuvaus	Kouluttaja esittelee Insafe-sivustoa etukäteen luodun sosiaalisen kirjanmerkkitilin avulla. Huomiota kiinnitetään oppilaille tarkoitettuihin neuvontapalveluihin (Helplines ja Hotlines) sekä opettajien sivuihin (Teacher Pages) ja lukuvuoden alkuun tarkoitettuihin materiaaleihin (Back to School). Kouluttaja kehottaa osallistujia tilaamaan uutiskirjeen. Kouluttaja esittelee nopeasti Safer Internet Day -sivustoa ja nostaa esiin digitaalisen turvallisuuden työkalupakit (eSafety Kits) tuntisuunnitelmineen ja opetusmateriaaleineen. Lopulta kouluttaja hakee Insafety-sivuston kautta joitakin osallistujien Safer Internet Awareness Centre (SIAC) -sivustoja ja tuo esiin, miten hyödyllisiä oppilaiden äidinkielellä toimivat SIAC-sivustot ovat kielen kehityksen kannalta. Kouluttaja esittelee osallistujille myös opetusmateriaalien jakamiseen tarkoitettu portaali Learning Resource Exchange ja sen Insafe-osio: http://lreforschools.eun.org **Käytännön tehtävä** Kouluttaja kysyy, käyttääkö kukaan osallistujista jo kirjanmerkkipalveluita, ja kertoo, että digitaalinen kirjanmerkkipalvelu helpottaa hyödyllisten linkkien ja materiaalien, kuten Insafe- ja Safer Internet Day -sivustojen, tallentamista. Tällaisia kirjanmerkkipalveluita ovat esimerkiksi Delicious ja Diigo. Kouluttaja esittelee interaktiivisella valkotaululla, kuinka Delicious-palveluun luodaan kirjanmerkkitili, ja auttaa osallistujia luomaan oman tilinsä. Tätä varten osallistujat tarvitsevat tilapäisen sähköpostiosoitteen.

	Jos joillain osallistujilla on jo kirjanmerkkitili, kouluttaja voi pyytää heitä avaamaan oppimisalustan tukimateriaaleista aineiston eS 1.5 Lista hyödyllisistä materiaaleista iän mukaan jaoteltuna ja lisäämään mielenkiintoiset materiaalit kirjanmerkkeihinsä. Uuden tilin luovat osallistujat tekevät saman sen jälkeen, kun heidän tilinsä on aktivoitu käyttöön. **Keskustelua** Osion päätteeksi kouluttaja voi kysyä kokeneilta kirjanmerkkien käyttäjiltä, mitä etua kirjanmerkeistä on opettajille ja oppilaille (todennäköisiä vastauksia ovat mm. seuraavat: hyödyllisyys erityisoppilaille, tiedon jakaminen, oppilaiden tiedonhaku tulee näkyväksi, hyödyllinen digitaalisten portfolioiden kokoamisessa, oppimispolun jäljittämisessä ja tekijänoikeuksien ja lähteiden merkitsemisessä). Digitaaliseen turvallisuuteen liittyvistä haittapuolista voi myös keskustella ryhmässä. Mahdollinen keskustelunaihe on myös se, kuinka edistää luokan tai oppiaineen yhteistä kirjanmerkkitiliä.
	Lounastauko, 1 tunti

Moduuli 1: KURSSIN TUKIMATERIAALIT

Nämä kurssin asiakirjat ovat tällä hetkellä saatavana erillisinä asiakirjoina.

Kurssi/Moduuli/Tehtävä	**Kurssin tukimateriaalit**
eS 1.1	Ihmisbingo digikansalaisille [tehtävämoniste]
eS 1.2	Digitaalisen turvallisuuden kurssin yleiskatsaus (pptx)
eS 1.3	Digitaalinen turvallisuus koulussa ja luokkaympäristössä (pptx)
eS 1.5	Luettelo hyödyllisistä materiaaleista iän mukaan jaoteltuna, 4–18-vuotialle [oppimisalustalla]

Kouluttajan käsikirja ja tukimateriaalit

Kurssi:

Digitaalinen turvallisuus: TURVALLISEMPI KOULU JA LUOKKAYMPÄRISTÖ

Moduuli 2: Digitaalista turvallisuutta nuorille ja opettajille

(eS 2.0)

eS 2.0: Digitaalista turvallisuutta nuorille ja opettajille

CPDLab-kurssi	**Digitaalinen turvallisuus: turvallisempi koulu ja luokkaympäristö**
Moduulin numero	**eS 2.0**
Moduulin nimi	**Digitaalinen turvallisuus nuorille ja opettajille**
Vaatimukset moduulin suorittamiseen	Tämä moduuli on tarkoitettu opettajille, jotka ovat jo suorittaneet moduulin 1 ja/tai heillä on perustiedot Internetiin, digitaaliseen mediaan ja digitaaliseen turvallisuuteen liittyvistä kysymyksistä. Moduulin 1 suorittaneet osallistujat ovat saaneet tietoa digitaaliseen turvallisuuteen liittyvistä parhaista käytännöistä kouluissa ja luokkaympäristössä. Osallistujat ovat luoneet tilin sosiaaliseen kirjanmerkkipalveluun ja tehneet moduulin 2 ennakkotehtävän ennen kurssia. • Luettele esimerkkejä erilaisista digitaaliseen turvallisuuteen liittyvistä kysymyksistä, joita oppilaat ja opettajat saattavat kohdata käyttäessään Internetiä, digitaalisia työkaluja, mobiililaitteita ja sosiaalista mediaa sekä koulussa että sen ulkopuolella. • Kuinka nämä digitaaliseen turvallisuuteen liittyvät kysymykset on otettu huomioon koulusi tietojärjestelmien käyttöehdoissa tai digitaalisen turvallisuuden toimintaohjeissa? **Huom.:** Kouluttajan tulee siirtää ryhmän digitaalisen turvallisuuden määritelmät tukimateriaalien diaan 9 pptx eS 2.1 ennen moduulin alkua.
Kesto	3 h
Kurssipaikka ja moduulin rakenne	• Tämä moduuli järjestetään lähiopetuksena. • Osallistujia kehotetaan ottamaan mukaan oma kannettava tietokoneensa. • Koko moduulin ajan osallistujat tutustuvat asioihin käytännössä ja voivat käyttää sosiaalista kirjanmerkkitiliään. • Lisäksi moduuliin kuuluu tehtäviä, keskustelua, ryhmätöitä ja pohdintaa. • Osallistujia rohkaistaan jatkuvasti etsimään ja valikoimaan materiaaleja ja linkkejä omalla äidinkielellään.
Tarvittavat tilat ja tilajärjestelyt	• Kouluttaja tarvitsee käyttöönsä kosketustaulun ja tietokoneen. • Osallistujat tarvitsevat käyttöönsä tietokoneen, jossa on Internet-yhteys. • Tiloissa tulisi olla tarpeeksi virtapistokkeita kannettaville tietokoneille. • Lisäksi osallistujat tarvitsevat tiloja, joihin hajaantua työskentelemään pieryh-

	missä.
Moduulin yleiskuvaus	Eurooppalaisten nuorten Internetin käytön vertailu. • Diginatiivi vs. digiosaaja? EU Kids Online -verkoston luokitus maittain. • Digitaalisen turvallisuuden kolme keskeistä osatekijää ("3Cs": contact, content ja conduct eli yhteydenotot, sisältö ja käytös): nuoret sisällön kuluttajina ja tuottajina. • Digitaalinen lukutaito ja digikansalaisuus: mitä ne tarkoittavat digitaalisen turvallisuuden kannalta? • Riskien ja mahdollisuuksien hallinta nuoren ja opettajan kannalta Kouluttajan tulisi moduulin aikana rohkaista osallistujia etsimään ja tallentamaan kirjanmerkkeihin materiaaleja ja palveluja omalla äidinkielellään.
Moduulin tavoitteet	• tunnistaa digitaalisen turvallisuuden kolmeen osatekijään ("3Cs") liittyvät riskit ja mahdollisuudet lasten ja nuorten osalta • ymmärtää, mitä tietoja, taitoja ja asenteita sekä opettajat että nuoret tarvitsevat digitaalista lukutaitoa ja turvallista verkon käyttöä varten • määritellä digitaalinen turvallisuus suhteessa digitaaliseen lukutaitoon ja digikansalaisuuteen • auttaa opettajia ymmärtämään, miten suojella yksityisyyttään ja verkkomainettaan.
Taitojen ja osaamisen karttuminen tässä moduulissa	Osallistujat oppivat • hallitsemaan Internetin turvallisuuteen liittyviä kysymyksiä ja etsimään paikallisia tukipalveluja tarkastelemaan koulun käytäntöjä ja arvioimaan niiden tehokkuutta • tunnistamaan digitaaliset kompetenssit, joita nuorten digitaaliseen turvallisuuteen vaaditaan • toteuttamaan digitaalisen turvallisuuden parhaita käytäntöjä opetuksessa ja oppimisessa • arvioimaan hyödyllisiä, opettajille ja kouluille tarkoitettuja, digitaalisen lukutaidon opetussuunnitelmaan ja digikansalaisuuteen liittyviä materiaaleja • etsimään digitaalisen turvallisuuden materiaaleja omalla äidinkielellään.
Tarvittavat materiaalit ja välineet	• eS 2.2a -monisteet • Kouluttajalle tietokone, jossa on Internet-yhteys, ja dataprojektori. • Kannettavat tietokoneet osallistujille • Langaton verkkoyhteys • Pääsy kurssin tukimateriaaleihin ja oppimispäiväkirjaan.
Vaatimukset kouluttajalle	• Kouluttajalla tulee olla syvällinen ja monipuolinen tietämys digitaalisesta lukutaidosta, digitaaliseen turvallisuuteen liittyvistä kysymyksistä ja digitaalisen turvallisuuden opetussuunnitelmista.

	• Kouluttajan tulee tuntea EU:n politiikka, joka tähtää Internetin parantamiseen lasten ja nuorten näkökulmasta, Insafe-verkoston materiaalit ja palvelut sekä paikallisen Safer Internet Centren aineistot, kansainväliset digitaalisen turvallisuuden opetussuunnitelmat ja kansainväliset digitaalisen lukutaidon ja digikansalaisuuden mallit. • Kouluttajalla tulee olla aikaa perehtyä paikallisiin tahoihin, jotka tarjoavat tukea kouluille ja opettajille digitaaliseen turvallisuuteen liittyvien ongelmatapausten yhteydessä. • Kouluttajan tulee tutustua kurssin verkkoalueeseen ja kaikkiin kurssin tukimateriaaleihin, jotka on lueteltu jokaisen moduulin lopussa. Jokainen materiaali on luetteloitu kurssin, moduulin ja tehtävän mukaan, esim. eS 1.1 Ihmisbingo digikansalaisille. Kouluttaja perustaa oppimisblogin ja antaa sen salasanan osallistujille. • Kouluttajan tulee käyttää sosiaalista kirjanmerkkipalvelua (esim. www.delicious.com tai Diigo www.diigo.com), jonne tallennetaan digitaaliseen turvallisuuteen liittyviä linkkejä ja materiaaleja. • Kouluttajan tulee myös kannustaa osallistujia luomaan oma käyttäjätilinsä, jonka avulla he voivat hallita kurssilla jaettuja verkko-osoitteita ja materiaaleja. • Kouluttajan tulee hallita blogisovellusten, etherpad-muistion, padlet-sovelluksen ja vastaavien käyttö.
Lähdeaineistoja ja materiaaleja kouluttajille	**Euroopan komissio** "Eurooppalainen strategia Internetin parantamiseksi lasten näkökulmasta", saatavana useilla eri kielillä: http://ec.europa.eu/information_society/activities/sip/policy/index_en.htm **Ammatillisen maineen vaaliminen** www.childnet.com/teachers-and-professionals/for-you-as-a-professional/professional-reputation **Insafe** www.saferinternet.org/online-issues/children-and-young-people Lasten ja nuorten verkon käyttöön liittyviä kysymyksiä.Tutkimustuloksia ja tapaustutkimuksia on saatavilla tukimateriaaleissa otsikolla **Byron Review** (eS 2. 2b Byron Review -raportti) . Monet lehtiotsikot havainnollistavat, miksi opettajat, aikuiset ja yhteiskunta yleensä suhtautuvat Internetiin varauksellisesti. Tämäntyyppisiä artikkeleita voi käyttää kuvaamaan asiaan liittyviä ongelmia, esim. www.tes.co.uk/article.aspx?storycode=6023305 yrittää selittää, miksi opettajat pelkäävät Facebookia. www.dailymail.co.uk/news/article-1354515/Teacher-sacked-posting-picture-holding-glass-wine-mug-beer-Facebook.html **Norjalaisen sanomalehden artikkeli:** www.dagbladet.no/2012/09/11/tema/nettsamfunn/Internett/facebook/sosiale_medier/23352303/. Kouluttajat ja osallistujat löytävät varmasti vastaavia esimerkkejä omalla kielellään.

Teachtoday-sivusto
www.teachtoday.eu/ Digitaaliseen turvallisuuteen liittyviä neuvoja opettajille, oppilaille ja vanhemmille.

Learning Resource Exchange -portaali ja sivuston Insafe-osio:
http://lreforschools.eun.org

EU Kids Online
Loppuraportti 2011:
www2.lse.ac.uk/media@lse/research/EUKidsOnline/EU%20Kids%20II%20(2009-11)/EUKidsOnlineIIReports/Final%20report.pdf
Internetin riskit ja turvallisuus verkossa:
www2.lse.ac.uk/media@lse/research/EUKidsOnline/EUKidsII%20(2009-11)/EUKidsOnlineIIReports/D4FullFindings.pdf

Byron Review –raportti
www.dcsf.gov.uk/byronreview "Safer Children in a Digital World" (Digitaalinen maailma turvallisemmaksi lapsille)

Teaching with technology in 2011 -raportti
www.teachtoday.eu/sitecore/shell/Applications/~/media/Files/United%20Kingdom/pdf/Teaching%20with%20technology%202011%20survey%20report%202011.ashx?db=master EUN:in julkaisema raportti tarjoaa kouluttajille yleiskatsauksen siitä, mitä tarpeita ja toiveita opettajilla on koulun ja luokkaympäristön digitaaliseen turvallisuuteen liittyen.

Digital competence for lifelong learning
ftp://ftp.jrc.es/pub/EURdoc/JRC48708.TN.pdf Euroopan komission tiedonanto, kirjoittajat Kirsti Ala-Mutka, Yves Punie and Christine Redecker 2008

Digitaalisen lukutaidon ja digikansalaisuuden opetussuunnitelma
www.commonsensemedia.org/educators Ilmainen opetussuunnitelma sekä opetus- ja oppimismateriaaleja kouluille ja opettajille. Commonsense Media - www.commonsensemedia.org/educators/curriculum

Digikansalaisuus: Turvallisuus, lukutaito ja etiikka digitaalisessa maailmassa
www.youtube.com/watch?feature=endscreen&v=h8YFAeCi8IA&NR=1 Video paneelikeskustelusta FOSI 2010 -konferenssissa.

Digikansalaisuus
www.ciconline.org/DigitalCitizenship Digitaalisen lukutaidon ja digikansalaisuuden opetussuunnitelma, Cable in the Classroom -järjestö, Yhdysvallat

	Nuorten digitaalinen elämä www.commonsensemedia.org/sites/default/files/research/socialmediasociallife-final-061812.pdf Common Sense Media -järjestön tutkimuksessa tarkastellaan sitä, kuinka nuoret näkevät oman digitaalisen elämänsä. **Sosiaalisen median hyvät ja huonot puolet luokkaympäristössä** www.zdnet.com/blog/igeneration/the-pros-and-cons-of-social-media-classrooms/15132 **Digitaalinen osaaminen ja digitaalinen lukutaito** http://linked.eun.org/web/guest/policyMaker Osittain Euroopan komission rahoittama projekti, joka tarkastelee tieto- ja viestintätekniikkaa hyödyntävän, innovatiivisen opetuksen ja oppimisen tutkimusta, politiikkaa ja käytäntöjä. **Connected Learning** http://clrn.dmlhub.net/resources/videos Monitieteinen tutkimusverkosto, tarkastelukohteena nykyisen muuttuvan mediaympäristön tarjoamat oppimismahdollisuudet ja toisaalta sen aiheuttamat riskit. **Internet-lukutaidon käsikirja The Internet Literacy Hand Book** www.coe.int/t/dghl/standardsetting/Internetliteracy/Source/Lit_handbook_3rd_en.swf **Tutkimus norjalaisten nuorten Facebookin käytöstä** www.slideshare.net/PetterB/social-implications-of-social-networking-sites
Arviointi-vaihtoehdot	• Ensimmäisen päivän oppimisen pohdinnassa osallistujat käyvät läpi päivän aikana oppimiaan asioita. Pohdinnassa voi myös mainita yhden turvallisuusstrategian, jonka he aikovat toteuttaa koulussaan. • Osallistujat käyttävät sosiaalista kirjanmerkkitiliään digitaaliseen turvallisuuteen liittyvien verkko-osoitteiden ja tukimateriaalien keräämiseen ja säilyttämiseen.
Moduulin jälkeiset jatkotoimenpiteet	Osallistujat voivat kokeilla parhaita käytäntöjä omissa kouluissaan ja raportoida edistymisestä toisilleen esim. kurssin jälkeen järjestettävässä webinaarissa. Jokainen osallistuja voi tarkistaa oman digitaalisen jalanjälkensä.
Vaihtoehtoiset tavat toteuttaa moduuli	Ei vaihtoehtoisia toteuttamistapoja.
Toteuttamis-vaihtoehdot kansallisella/ paikallisella	Tämä moduuli voidaan toteuttaa kansallisella/paikallisella tasolla. Kuten kaikessa jatkokoulutuksessa, voi olla hyödyllistä koota ryhmään eri maakunnista/alueilta tulevia ihmisiä jakamaan kokemuksiaan. Kurssin jälkeen kouluttaja voi pitää jatkowebinaarin, jossa osallistujat pääsevät keskustelemaan siitä, kuinka he ovat soveltaneet opetukses-

tasolla	saan kurssin asioita ja kuinka niitä on toteutettu koulussa yleisesti.
Tehtävä 2.1	**Digitaalinen lukutaito ja digikansalaisuus – mitä ne merkitsevät digitaalisen turvallisuuden kannalta?**
Kesto	55 min
Tavoitteet	• Ymmärtää, kuinka nuoret käyttävät Internetiä arjessaan. • Tunnistaa digitaalisen lukutaidon opettamisen tarve. • Ymmärtää, miten digitaalinen lukutaito ja digikansalaisuus muodostavat osan digitaalista turvallisuutta. • Tarkastella sitä, miten koko koulun digitaalisen lukutaidon opetussuunnitelmalla voidaan suojata oppilaita ja auttaa heitä kehittämään omaa vastuullisuuttaan digitaalisen median käyttämisessä. • Keskustella koko koulun digitaalisen turvallisuuden strategioista ja ratkaisuista riskien pienentämiseksi.
Kuvaus	Kouluttaja käyttää materiaalissa eS 2.1 Digitaalinen turvallisuus ja digitaalinen lukutaito pptx olevia lisämuistiinpanoja ja toimii seuraavasti: • **@ Dia 3** Kouluttaja näyttää videon, jossa esitetään viimeisimmän tutkimustiedon perusteella lyhyt yhteenveto lasten ja nuorten ajanvietosta verkossa www.youtube.com/watch?v=a8J06gVIR8o, ja pyydä osallistujilta kommentteja. • **@ Diat 5 & 6** Kouluttaja näyttää EU Kids Online -verkoston maakohtaiset tilastot, jotka korostavat digitaalisen lukutaidon opettamisen tarvetta. Kouluttaja esittelee joitain tutkimustuloksia ja tapaustutkimuksia, jotka käsittelevät digitaaliseen lukutaitoon liittyviä kysymyksiä. Vuonna 2010 tehdyssä EU Kids Online -tutkimuksessa määritettiin kahdeksan digitaaliseen lukutaitoon ja turvallisuuteen liittyvää taitoa ja arvioitiin, ovatko lapset ja nuoret oppineet nämä taidot tiettyyn ikään mennessä. Tulokset sisältävät maakohtaisen listauksen. Ne ovat mielenkiintoinen tapa esitellä digitaalisen lukutaidon käsite ja perustella sen tärkeyttä. (Kouluttajalle on saatavilla tukimateriaali eS 2.1a Digitaalisen median lukutaito.) • **@ Dia 7** Kouluttaja näyttää lainauksen Euroopan komission materiaalista, jossa todetaan, että myös opettajat tarvitsevat digitaalista osaamista voidakseen tukea oppilaita. Kurssin tavoitteena on antaa opettajille uutta digitaalista osaamista, jotta he voivat hyödyntää digitaalisen teknologian tarjoamia mahdollisuuksia ja puuttua digitaalisen turvallisuuden ongelmiin kouluissaan.

- **@ Dia 8**
  Kouluttaja napsauttaa kohtaa 'literate, safe, ethical citizens' (lukutaitoiset, suojatut, eettiset käyttäytyvät kansalaiset) käynnistääkseen **videon** 'What is Digital Citizenship?' (Mitä digikansalaisuus tarkoittaa?)
  http://www.youtube.com/watch?v=e0I13tKrxcA

  Digitaalinen lukutaito on arjen taito, joka ei liity itse teknologiaan vaan siihen, miten teknologiaa käytetään. Digitaalinen lukutaito auttaa vanhempia vanhemmuudessa ja opettajia työssään. Se on nykypäivän lukutaitoa ja osa kansalaistaitoja nyt ja tulevaisuudessa.

- **@ Dia 9**
  Kouluttaja on siirtänyt ryhmän digitaalisen turvallisuuden määritelmät dialle lounastauon aikana. Kouluttaja kysyy: Tänä aamuna määrittelimme, mitä digitaalinen turvallisuus tarkoittaa omalla kohdallamme. Kuinka onnistuimme? Keskustelua määrittelyissä esiintyvistä keskeisistä piirteistä. Kouluttaja kysyy, kuinka henkilökohtainen turvallisuus, digitaalinen lukutaito ja digikansalaisuus voidaan nähdä osana digitaalista turvallisuutta?

- **@ Dia 10**
  Osallistujat **keskustelevat** oman maansa tieto- ja viestintätekniikan viitekehyksestä (nimi voi vaihdella maan mukaan) ja kuinka nykyaikana tarvitaan uudenlaista lukutaitoa: perinteisen luku- ja laskutaidon lisäksi oppilaat tarvitsevat digitaalista lukutaitoa. Keskustelkaa siitä, mitä tämä tarkoittaa.

- **@Dia 11 & 12**
  Ryhmätyö (3–4 hengen pienryhmissä), tarkastellaan yhtä neljästä digitaalisen lukutaidon opetussuunnitelmasta.

  Jokainen pienryhmä esittää yhteenvedon keskustelustaan koko ryhmälle haluamallaan tavalla. Digitaalista turvallisuutta voidaan opettaa systemaattisesti koko koulua koskevan opetussuunnitelman avulla. Kouluttaja voi kertoa osallistujille, että koko koulun digitaalisen turvallisuuden toimintasuunnitelmia käsitellään moduuleissa 9 ja 10 (Päivä 5).

  Kouluttaja tiivistää yleisen keskustelun aikana osallistujien keskeisimmät kokemukset digitaalisen lukutaidon opetussuunnitelmasta.

Tehtävä 2.2	**Riskit ja mahdollisuudet**
Kesto	45 min
Tavoitteet	Saada erilaisia näkökulmia oppilaiden ja opettajien Internetin käyttöön.
Kuvaus	Kouluttaja näyttää aineiston eS 2.2 Riskit ja mahdollisuudet ppt

- **@ Dia 2**
  Kouluttaja selittää Internet-turvallisuuden kolme keskeistä osatekijää ("3Cs",

englannin sanoista contact, content ja conduct eli yhteydenotot, sisältö ja käytös): ne voivat edustaa sekä riskejä että mahdollisuuksia, mutta varsin usein koulut näkevät nuorten digitaalisen teknologian käytössä vain riskejä. Syynä tähän on pelon kulttuuri, joka ympäröi Internetin käyttöä kouluissa. Internetin ensimmäisen vaiheen aikana kaikki olivat vain verkossa olevan tiedon kuluttajia. Siihen aikaan huolta aiheuttivat yhteydenottoihin (Contact) liittyvät riskit (enimmäkseen vieraiden ihmisten ja pedofiilien aiheuttamat vaarat). Nykyisin Internetin vuorovaikutteinen ja mobiili luonne sekä nopeat verkkoyhteydet mahdollistavat epäsopivat ja riskialttiit yhteydenotot lasten välillä (virtuaalinen kiusaaminen, tahallinen provosointi eli "trollaus", seksuaalissävytteisten kuvien ja viestien lähettäminen tai tuntemattomien henkilöiden tapaaminen).

Tiedoksi kouluttajille: Toista sama sisällön (*Content)* ja käytöksen (*Conduct)* kohdalla.

- **@ Dia 5**
  Mitä digitaalinen turvallisuus tarkoittaa.
- **@ Dia 10**
  Kouluttaja kysyy osallistujilta heidän näkemyksiään vanhempien roolista. Miten olla vanhempi nykyaikana? Vanhempien tulee ymmärtää lasten teknologian käyttöön liittyviä kysymyksiä, tuntea todelliset riskit ja käyttäytyminen ja oppia yksinkertaisia strategioita, joiden avulla lapsi on paremmin turvassa. Kuinka koulut voivat auttaa vanhempia?
  Tehtävä: Osallistujat menevät Safer Internet Awareness Centren verkkosivuille, tutkivat niitä ja raportoivat sen pohjalta: Mitä materiaaleja tai palveluja heidän oman maansa Safer Internet Awareness Centre tarjoaa vanhemmille? Verkkosivustoihin tutustumiseen tulee varata hetki aikaa.
- **@ Diat 12 -14**
  Millaista riskialtista verkkokäyttäytymistä maassasi esiintyy?
- **@ Diat 16 – 18**
  Keskustelua sosiaalisiin verkostoihin liittyvistä huolenaiheista.
- **@ Dia 19**
  Keskustelua. Kouluttaja kysyy, onko kukaan käyttänyt eTwinning-alustaa (ilmainen, koko Euroopan kattava sosiaalisen oppimisen alusta, joka on tarkoitettu myönteisen sosiaalisen oppimisen ja viestinnän opettamiseen). Kouluttaja esittelee alustan lyhyesti. Voisiko turvallisten sosiaalisen oppimisen työkalujen käyttö auttaa hallitsemaan joitain sosiaaliseen mediaan liittyviä riskejä kouluissa?
- **@ Dia 20**
  Kouluttaja pitää loppukeskustelun näytettyään bloggauksesta kertovan videon, joka on linkitetty 'opettajat' sanaan. Kenen tulisi opettaa bloggausta?
  Moniste eS2.2a Mallia sosiaalisen median käyttöön (pdf) jaetaan osallistujille. Keskustelkaa kohdasta kahdeksan ja muista kohdista, jotka liittyvät kunnioitta-

	van käytöksen mallin näyttämiseen, erityisesti sosiaalisessa mediassa käytettävän kielen ja keskustelun osalta. Pdf on peräisin Irlannin opetusministeriön uudesta kiusaamista koskevasta toimintasuunnitelmasta (Action Plan on Bullying, Dept. of Education Ireland 2013). (Kiusaamista käsitellään moduulissa 6) Kuka voi näyttää mallia sosiaalisen median työkalujen turvallisesta ja kunnioit tavasta käytöstä? Kouluttaja kysyy, kenen koulussa on käytössä virtuaalinen oppimisympäristö tai oppimisalusta. Voiko sitä käyttää opetuksessa? Koulutta ja pyytää osallistujilta ehdotuksia ja esimerkkejä, miten he hyödyntävät oppi – misalustaa. Kouluttaja etsii turvallisia ja hyödyllisiä työkaluja, jotka tehostavat opetusta ja oppilaiden oppimista ja pyytää ehdotuksia turvallisista työkaluista. Kuinka voimme tarjota oppilaille välineet (esim. etiketti, kunnioitus) sosiaalisen median käytön hallitsemiseen? Näitä kysymyksiä ja strategioita niiden käsitte lyyn tarkastellaan kurssin muissa moduuleissa.
	Kahvitauko 10 min
Tehtävä 2.3	**Internetin turvallinen käyttö**
Kesto	55 min
Tavoitteet	• Löytää ratkaisuja, joiden avulla nuoret ja opettajat voivat käyttää Internetiä turvallisesti. • Tunnistaa omaan sosiaalisen median käyttöön liittyvät riskit.
Kuvaus	Kouluttaja pitää esityksen eS 2.3 Internetin turvallinen käyttö pptx kartoittaakseen opettajien asenteita ja pelkoja sekä ratkaisuja tieto- ja viestintätekniikan vastuulliseen käyttöön. • **@ Dia 3** Kouluttaja avaa seuraavan linkin: www.childnet.com/teachers-and-professionals/for-you-as-a-professional/using-technology . Osallistujat tarkastelevat pienryhmissä "At School"- ja "In the Classroom"-osioita. Aluksi katsotaan kuitenkin " At Home"-osion kysymyksiä ja vastauksia *Using Technology* -sivulla. 1) Ensimmäinen kysymys käsittelee VERKON KÄYTTÖÄ – oman digitaalisen jalanjäljen poistaminen ja yksityisyysasetuksien tarkistaminen yhteisöpalvelusivustoilla. Ovatko neuvot merkityksellisiä ryhmän kannalta? 2) Toinen kysymys käsittelee MOBIILIKÄYTTÖÄ – PIN-koodien ja salasanojen suojaaminen ja tietokoneilta uloskirjautumisen tärkeys. Onko tämä neuvo merkityksellinen myös oppilaiden kannalta? Kuinka tätä voidaan opettaa? **Tiedoksi kouluttajille, ryhmätyö:** Kouluttaja jakaa sivuston osioiden "At School" ja "In the Classroom" kysymykset ja vastaukset kolmihenkisille ryhmille, 2 – 3 kysymystä ja

vastausta per pienryhmä. Ryhmien tehtävänä on päättää, ovatko neuvot sopivia opettajille heidän omassa maassaan. Sen jälkeen ryhmä voi tehdä lisäyksiä ja parannella neuvoja näkemyksensä mukaan.

Palaute

Ryhmät luovat etherpad-sivun (esim. Etherpad: http://etherpad.opensourcebridge.org tai http://openetherpad.org) ja kirjaavat vastauksensa sinne yhdessä. Jokainen ryhmä jakaa etherpad-sivunsa interaktiivisella valkotaululla ja avaa digitaaliseen turvallisuuteen liittyviä kysymyksiä, joita opettajat käsittelivät heille jaetuissa kysymyksissä ja vastauksissa. Mitä käytäntöjä heidän omissa kouluissaan on henkilöstön tueksi? Antaako opetusministeriö tai vastaava taho kansallisen tason ohjausta? Onko olemassa ammatillisia toimintaohjeita? Voivatko osallistujat etsiä linkkejä yllämainittuihin ja lisätä ne sosiaalisiin kirjanmerkkeihinsä?
Keskustelkaa osallistujien vastauksista.
Mitä mieltä ryhmä on ammatillista mainetta koskevista neuvoista sivulla www.childnet.com/teachers-and-professionals/for-you-as-a-professional/professional-reputation . Kouluttaja kertoo, että linkin @ www.childnet.com/teachers-and-professionals/for-you-as-a-professional/professional-reputation takana on kysymyksiä ja vastauksia opettajille Britanniassa. Osallistujien tulisi tallentaa se kirjanmerkkeihin myöhempää tutustumista varten.

- **@ Dia 4**
  Ryhmäkeskustelu akvaariomenetelmän avulla. Osallistujat jaetaan kahteen ryhmään.

1) Ensimmäinen ryhmä keskustelee aluksi 5–10 minuutin ajan seuraavasta aiheesta: Kuinka nuoret voivat käyttää Internetiä turvallisesti?
   Toinen ryhmää seuraa keskustelua, mutta ei osallistu siihen. He voivat tehdä muistiinpanoja keskustelusta ja kommentoida sitä lyhyesti keskustelun jälkeen.
2) Seuraavaksi ryhmät vaihtavat rooleja. Seuraava vaihe on muuten samanlainen, mutta ryhmä keskustelee seuraavasta aiheesta: Kuinka opettajat voivat käyttää Internetiä turvallisesti opetustarkoituksiin luokkaympäristössä?

   Tämän jälkeen seuraa kymmenen minuutin keskustelu koko ryhmän kanssa molemmista aiheista. Lopuksi kouluttaja esittää yhteenvedon kaikkien keskustelujen pääasioista.

Tehtävä 2.4	**Yhteenveto – opittavat asiat ja pohdintaa**
Kesto	15 min
Tavoitteet	• Tehdä yhteenveto osallistujien päivän aikana oppimista asioista. • Pohtia omaa oppimista verkkoon kirjoitettavassa oppimispäiväkirjassa.

Kuvaus	Kouluttaja esittää tiivistetysti joitain pääkohtia, joita on käsitelty päivän aikana. Osallistujat kirjoittavat oppimispäiväkirjaansa ajatuksiaan ja pohdintojaan koulutuspäivästä ja siitä, mitä he aikovat tehdä jatkossa.

Moduuli 2: KURSSIN TUKIMATERIAALIT

Yhteenveto kouluttajan tarvitsemista tukimateriaaleista, joita käytetään ylläkuvatun moduulin tehtävien ohjaamisessa.

Kurssi/Moduuli/Tehtävä	**Kurssin tukimateriaalit**
eS 2.1	eS 2.1 Digitaalinen turvallisuus ja digitaalinen lukutaito (pptx)
eS 2.2	eS 2.2 Riskit ja mahdollisuudet pptx
eS 2.2a	eS2.2a Mallia sosiaalisen median käyttöön (pdf) [jaettavaksi]
eS 2.3	eS 2.3. Internetin turvallinen käyttö (pptx)
Tukimateriaalia	Nämä aineistot voi lisätä kurssin verkko-oppimisympäristöön tai oppimisalustalle.
eS 2.1a	eS 2.1a Digitaalisen median lukutaito (pdf)
eS 2.2b	eS 2. 2b Byron Review -raportti (pdf)

Kouluttajan käsikirja ja tukimateriaalit

Kurssi:

Digitaalinen turvallisuus: TURVALLISEMPI KOULU JA LUOKKAYMPÄRISTÖ

Moduuli 3: Digitaalisen turvallisuuden taidot: digikansalaisuus

(eS 3.0)

eS 3.0: Digitaalisen turvallisuuden taidot: Digikansalaisuus

CPDLab-kurssi	**Digitaalinen turvallisuus: Digitaalisen turvallisuuden parantaminen kouluissa**
Moduulin numero	**eS 3.0**
Moduulin nimi	**Digitaalisen turvallisuuden taidot: digikansalaisuus**
Vaatimukset moduulin suorittamiseen	Osallistujilla tulee olla perustaidot tieto- ja viestintätekniikan käytössä ja kiinnostus digitaalisen teknologian ja Internetin käyttöön opetuksessa ja oppimisessa. Heillä tulee olla jonkinlainen tuntemus sosiaalisen median palveluista, niiden toiminnasta ja käytöstä. Ihanteellista olisi, jos osallistujat ovat suorittaneet moduulit 1 ja 2. Heidän tulisi olla kiinnostuneita siitä, miten sosiaalisen median interaktiiviset pedagogiset työkalut, kuten eTwinning, virtuaaliset oppimisympäristöt, oppimisalustat tai Edmodo, voivat tehostaa opetusta ja oppimista, kun opettaja näyttää mallia ja moderoi työkalujen käyttöä. Osallistujat tarvitsevat tilapäisen sähköpostiosoitteen (ei henkilökohtaista osoitetta tai koulun tai työpaikan sähköpostiosoitetta), jota he voivat käyttää kokeillakseen erilaisiin sosiaalisen median palveluihin rekisteröitymistä ja niiden käyttöä. Heillä tulisi olla moduulin 1 aikana perustettu tili sosiaalisessa kirjanmerkkipalvelussa ja pääsy oppimisblogiin ja kurssin tukimateriaaleihin.
Kesto	3 tuntia
Kurssipaikka ja moduulin rakenne	• Tämä moduuli järjestetään lähiopetuksena. • Osallistujia kehotetaan ottamaan mukaan oma kannettava tietokoneensa, sillä moduulin aikana kokeillaan opetettavia asioita käytännössä. • Sen lisäksi moduuli sisältää tehtäviä, keskustelua ja ryhmätöitä. • Osallistujia rohkaistaan jatkuvasti etsimään ja valikoimaan materiaaleja ja linkkejä omalla äidinkielellään.
Tarvittavat tilat ja tilajärjestelyt	• Kouluttaja tarvitsee käyttöönsä kosketustaulun, tietokoneen ja langattoman verkon. • Osallistujat tarvitsevat käyttöönsä tietokoneen, jossa on Internet-yhteys. • Tiloissa tulisi olla tarpeeksi virtapistokkeita kannettaville tietokoneille. • Lisäksi osallistujat tarvitsevat tiloja 3–5 hengen pienryhmätyöskentelyyn.

Moduulin yleiskuvaus	Sosiaalisesta mediasta on tullut keskeinen osa ihmisten elämää. Tässä moduulissa kouluttaja esittää esimerkkejä yleisimmistä sosiaalisen median palveluista ja mobiilipalveluista. Osallistujilla on mahdollisuus oppia, kuinka maksimoidaan sosiaalisen median myönteinen, turvallinen käyttö ja minimoidaan väärinkäytön vaarat. Moduulin aikana keskustellaan näihin palveluihin liittyvistä digitaalisen turvallisuuden kysymyksistä ja tarkastellaan erilaisia riskienhallintastrategioita. Opettajat voivat näyttää mallia sosiaalisen median parhaista käytännöistä oppilaille. Näin voidaan opettaa digikansalaisuutta ja digitaalista lukutaitoa käyttämällä tehtäviin perustuvia opetustyökaluja, kuten eTwinningiä. Moduulissa kartoitetaan sosiaalisen median ja mobiililaitteiden tarjoamia oppimismahdollisuuksia ja haittapuolia luokkaympäristössä. Sosiaalista mediaa opetuksessa käyttäville opettajille annetaan mahdollisuus kertoa, kuinka he käyttävät sosiaalisen median palveluja. ETwinning-alustan tai ilmaisen virtuaalisen oppimisympäristön (Edmodo tai vastaava) käyttäjät voivat esitellä ryhmälle niiden pedagogista käyttöä. Keskustellaan ryhmässä koko koulun yhteisten käytäntöjen tarpeesta sosiaalisen median käytössä. Lisäksi käsitellään oman teknologian tuomista kouluun (BYOT) ja sen vaatimia turvallisuusjärjestelyjä koko koulussa. (Lisää oman teknologian käytöstä moduulissa 9.) Tarkastellaan digikansalaisuuden lisäämistä opetussuunnitelmaan ja vastuullisen sosiaalisen median käytön opettamista ja oppimista. Moduulissa käsitellään sosiaalista mediaa opettajien ammatillisen kehittymisen työkaluna sekä opetus- ja oppimistyökaluna, jonka avulla osallistetaan oppilaita.
Moduulin tavoitteet	• Sosiaalisen median voiman ja hyödyllisyyden ymmärtäminen oppimisessa ja elämässä yleensä. • Sosiaalisen median turvalliseen käyttöön liittyvien ongelmien tunnistaminen ja käyttäjien suojaaminen mahdollisilta riskeiltä. Tähän kuuluvat sekä oppilaita että opettajia koskevat riskit. • Joidenkin sosiaalisen median työkalujen ja palvelujen käyttäminen, pedagogisista periaatteista keskusteleminen ja pohdinta siitä, kuinka näitä työkaluja ja palveluja voidaan turvallisesti käyttää perinteisten opetuskäytäntöjen lisänä. • Koko kouluyhteisön ymmärtämien ja hyväksymien, selkeiden sosiaalisen median käytäntöjen tarpeellisuuden ymmärtäminen. • Sosiaalisen median käyttäminen ammatillisessa kehittymisessä.
Taitojen ja osaamisen karttuminen tässä moduulissa	Osallistujat oppivat • käyttämään sosiaalisen median palveluja ja työkaluja turvallisemmin • ymmärtämään sosiaalisen median opetuskäytön edut ja haasteet • tunnistamaan pedagogiset periaatteet, joiden perusteella voidaan käyttää interaktiivisia digitaalisia työkaluja opetuksessa ja jatkuvassa ammatillisessa kehittymisessä • tukemaan oppilaiden oppimista ja osallisuutta digitaalisten sosiaalisten oppimistyökalujen kautta.

Tarvittavat materiaalit ja välineet	• Kurssin sisältö, oppimispäiväkirja ja verkkofoorumi ryhmän oppimisalustalla. eS 3.2a -osion moniste. • Kouluttajalle tietokone, jossa on Internet-yhteys, ja dataprojektori. • Osallistujille kannettavat tietokoneet ja pääsy langattomaan verkkoon. • Kosketustaulu tulosten esittämiseen. Pääsy kurssin tukimateriaaleihin ja oppimispäiväkirjaan. • Osallistujille tulisi jakaa mahdollisuuksien mukaan paperikopio materiaalista "*Using the mobile phone in school*". Materiaali on saatavilla myös seuraavan linkin kautta: http://lreforschools.eun.org/web/guest/resource-details?resourceId=407595 . Kouluttajan tulee myös jakaa materiaali eS 3.2a Esimerkki mobiililaitteiden käyttösäännöistä siihen liittyvän tehtävän aikana.
Vaatimukset kouluttajalle	Kouluttajien tulisi tuntea joitain sosiaalisen median palveluja ja työkaluja sekä pystyä esittelemään ja käyttämään niitä. Minimivaatimuksena on, että kouluttaja pystyy keskustelemaan Facebookista ja Twitteristä asiantuntevasti, sillä ne ovat kaksi suosituinta verkkoyhteisöpalvelua. Kouluttajan tulisi ymmärtää yleisiä sosiaaliseen mediaan ja mobiilityökaluihin, kuten blogeihin, wikeihin, Facebookiin, Twitteriin, Appseihin, YouTubeen, Googlen työkaluihin, tiedostonjako-ohjelmiin (kuva-, video-, ääni- ja musiikkitiedostot) ja sijaintipalveluihin (GPS), liittyviä yleisiä digitaalisen turvallisuuden ongelmia. Kouluttajan tulee pystyä johtamaan keskustelua ilmaisten yhteisöllisten oppimistyökalujen hyödyllisestä opetuskäytöstä (esimerkiksi eTwinningin Twinspace, Schoology ja Edmodo tai vastaavat) ja esittelemään turvallisia sosiaalisen median oppimiskäyttöön tarkoitettuja sivustoja. Kouluttajan tulee kerätä ideoita ja kommentteja osallistujilta ja johtaa keskustelua niiden pohjalta. Mikäli mahdollista, kouluttajan tulee rekisteröityä sekä eTwinningiin että Edmodoon ennen kurssia ja esitellä niiden ominaisuuksia kosketustaululla. Kouluttajien tulee tutustua kurssin verkkoalueeseen ja kaikkiin kurssin tukimateriaaleihin, jotka on lueteltu jokaisen moduulin lopussa. Jokainen materiaali on luetteloitu kurssin, moduulin ja tehtävän mukaan, esim. eS 1.1 Ihmisbingo digikansalaisille, ja moduulin aikana käytetään omaa sosiaalista kirjanmerkkitiliä materiaalien hakemiseen.
Viitetiedot ja materiaalit kouluttajille	Lista sosiaalisen median palveluista verkko-osoitteineen. Aikarajoitusten vuoksi kouluttajien täytyy valita ryhmän kannalta tärkeimmät palvelut; Facebook ja Twitter ovat kaksi suosituinta verkkoyhteisöpalvelua. Opettajat voivat käyttää Twitteriä oman jatkuvan ammatillisen kehityksensä välineenä. www.twitter.com www.facebook.com www.eTwinning.org www.edmodo.com (tai vastaava) **Muita vaihtoehtoja:** www.youtube.com www.google.com (Google+) Apps (katso www.scoilnet.ie/parents_apps_safety1.shtm ja www.schrockguide.net/bloomin-apps.html)

Kurssin lokalisointia varten voi mahdollisesti käyttää paikallisia verkkoyhteisöpalveluja: esim. www.rebelmouse.com Hi 5, Habbo Hotel ....
Muita palveluja tai sovelluksia: Snapchat, Ask.fm, Chat Roulette

Materiaalia/työkaluja kouluttajalle:

Sosiaalisen median hyvät ja huonot puolet luokkaympäristössä
www.zdnet.com/blog/igeneration/the-pros-and-cons-of-social-media-classrooms/15132

Hallitse verkkotunnuksiasi
www.slideshare.net/clifmims/managing-online-identities-tips-for-teachers-students-and-parents

Hallitse ammatillista mainettasi
www.childnet.com/teachers-and-professionals/for-you-as-a-professional/professional-reputation

Miksi verkkoyhteisöpalveluissa toimimisen taitoja on tarpeen opettaa
www.thethinkingstick.com/why-we-need-to-teach-social-networking

Turvallisuusneuvoja vanhemmille sovellusten käytöstä
www.scoilnet.ie/parents_apps_safety1.shtm

Kathy Schrockin luokittelemat opettajille tarkoitetut sovellukset
www.schrockguide.net/bloomin-apps.html

60 tapaa käyttää Twitteriä luokkaympäristössä kategorioittain
www.teachthought.com/social-media/60-ways-to-use-twitter-in-the-classroom-by-category/

10 parasta blogia – ehdotettu Twitterissä seurattavaksi
www.educatorstechnology.com/2012/11/top-10-educational-technology-blogs-for.html

Matkapuhelimen käyttäminen oppimisvälineenä koulussa
http://lreforschools.eun.org/web/guest/resource-details?resourceId=407595

25 sosiaalisen median vinkkiä opettajille
www.teachthought.com/social-media/25-social-media-tips-youve-probably-never-heard/

Digizen
www.digizen.org Sivustolla on neuvoja ja materiaaleja, jotka käsittelevät esimerkiksi verkkoyhteisöpalveluja ja virtuaalista kiusaamista, sekä sitä, kuinka ne liittyvät ja vaikuttavat ihmisten omaan ja muiden verkkokäyttäytymiseen ja kokemuksiin.

Strategioita sosiaalisen median käyttöön luokkaympäristössä
http://gettingsmart.com/blog/2011/12/developing-a-social-media-strategy-for-your-classroom/

Kuinka luoda sosiaalisen median ohjeet kouluille
www.edutopia.org/how-to-create-social-media-guidelines-school

Know it all
www.childnet.com/kia/ Britannian Childnet-sivuston opetusaineistoja, jotka on suunniteltu valistamaan vanhempia, opettajia ja nuoria Internetin turvallisesta ja myönteisestä käytöstä.

Think you know?
www.thinkuknow.co.uk/Teachers/ Aineistoja opettajille, oppilaille ja vanhemmille. Vaatii rekisteröitymisen.

Facebookin hyödyllinen käyttö oppimisessa
http://edudemic.com/2012/09/amsterdam-school-facebook-timeline-history-classes/?goback=.gde_138011_member_199774561

www.fbparents.org Loistava opas Facebookin käyttöön – tarkoitettu vanhemmille, mutta antaa myös hyvän yleiskuvan palvelusta

www.facebook.com/safety/attachment/Guide%20to%20Facebook%20Security.pdf

Humoristinen katsaus Facebook-käytökseen
http://socialmediatoday.com/daniel- zeevi/1312321/11-things-you-need-immediately-stop-doing-facebook

European Schoolnet's Smile Project (Social Media in Learning & Education)
www.eun.org/web/guest/projects/current/-/asset_publisher/Vy6l/content/125737?_101_INSTANCE_Vy6l_redirect=%2Fweb%2Fguest%2Fprojects%2Fcurrent

eS 3.1f Google Plus ja ammatillisen identiteetin suojaaminen doc Neuvoja opettajille Google Plus -palvelun käyttöön

Lisälukemista:
Digital tools, digital classrooms – Web 2.0 new tools, new schools (Gwen Solomon, Lynne Schrum; iste 2007)
The Socially Networked Classroom – teaching in the new media age (William Kist; Corwin 2010)
Teaching with the tools kids really use – Learning with web and mobile technologies (Susan Brooks-Young; Corwin 2010)
Blogs, Wikis, Podcasts and other powerful web tools for classrooms (Will Richardson; Corwin 2006)
Net Smart How to Thrive Online, Rheingold, Howard; Weeks, Anthony (2012-02-24) Net Smart MIT Press. Kindle Edition

Arviointi-vaihtoehdot

- Ryhmä perustaa Twitter-kanavan, ja jokainen osallistuja twiittaa kerran päivässä loppukurssin ajan.
- Osallistujat tallentavat verkkosivustoja ja linkkejä sosiaaliselle kirjanmerkkitililleen.

Moduulin jälkeiset jatkotoimenpiteet	Yhteen kerättynä ryhmän pedagogiset ideat muodostavat ideapankin, jota osallistujat voivat hyödyntää ja kokeilla ideoita omissa luokissaan. Osallistujat voivat pitää yhteyttä kurssin jälkeen sosiaalisen median (esim. Twitter-kanavan) kautta.
Vaihtoehtoiset tavat toteuttaa moduuli	Paikallisesti järjestetty kurssi voidaan toteuttaa siten, että osallistujat ehdottavat etukäteen materiaaleja ja sosiaalisen median alustoja, joita he haluaisivat käsitellä kurssilla. Tämä riippuu tietysti siitä, miten paljon kouluttajalla on aikaa käytettävissä, ja onko käytännöllistä keskittyä yhteisöpalveluun, jota käytetään vain yhdessä tai kahdessa maassa. Tästä syystä suosittelemme, että moduuli perustuu esimerkiksi Facebookin ja Twitterin tai vastaavien palveluiden käsittelyyn. Opettajille tulisi esitellä sosiaalisen median, kuten esimerkiksi eTwinningin tai Edmodon, käyttöä hyödyllisiin opetustarkoituksiin.
Toteuttamisvaihtoehdot kansallisella /paikallisella tasolla	Tämä moduuli voidaan toteuttaa kansallisella/paikallisella tasolla. Moduulista voidaan toteuttaa myös rehtoreille ja päätöksentekijöille räätälöity versio, jossa huomio kohdistuu enemmän koko koulun käytäntöihin ja turvallisuussääntöihin. Kouluttaja esittelee palveluja ja niiden keskeisiä ominaisuuksia digitaalisen turvallisuuden näkökulmasta: moduulissa voidaan keskittyä esimerkiksi kahteen maailmanlaajuisesti käytettyyn julkiseen sivustoon ja kahteen opetussivustoon, joissa on sosiaalisen median toimintoja ja jotka ovat turvallisuusominaisuuksiltaan sopivia opetuskäyttöön. Twitter on hyvä verkostoitumistyökalu rehtoreille. Tätä kohderyhmää varten kouluttajan tulee lisätä moduuliin sisältöä, joka käsittelee sosiaalisen median ohjeita, omien laitteiden käyttöön liittyviä käytäntöjä, digitaaliseen turvallisuuteen liittyvien ongelmatapausten käsittelyä ja kouluja koskevia oikeudellisia kysymyksiä sekä vanhempien osallistamista. Näitä asioita käsitellään moduuleissa 9 ja10.
Tehtävä 3.1:	**Digitaalinen turvallisuus ja sosiaalisen median työkalut**
Kesto	1 h 40 min
Tavoitteet	• Tutustua erilaisiin sosiaalisen median palveluihin, mobiilityökaluihin ja sovelluksiin. • Ymmärtää sosiaalisen median ja mobiilityökalujen käyttöön liittyviä digitaalisen turvallisuuden ongelmia. • Tarkastella, miten vastuullisen käytön ja digikansalaisuuden opettaminen voi pienentää digitaalisia turvallisuusriskejä. • Tarkastella, miten sosiaalisen median työkaluilla voidaan tehostaa opetusta, oppimista ja opettajien ammatillista kehitystä.
Kuvaus	Kouluttaja esittelee palveluja ja niiden keskeisiä ominaisuuksia digitaalisen turvallisuuden näkökulmasta: moduulissa voidaan keskittyä esimerkiksi kahteen maailmanlaajuisesti käytettyyn julkiseen sivustoon ja kahteen opetussivustoon, joissa on sosiaalisen median toimintoja ja jotka ovat turvallisuusominaisuuksiltaan sopivia opetuskäyttöön. 1. Facebook 2. Twitter 3. eTwinningin Twinspace

4. Edmodo (tai vastaava)

Muita vaihtoehtoja:

5. Google +
6. Lokalisoitu materiaali (Kun kurssi lokalisoidaan, kouluttaja voi valmistella sopivan materiaalin)

Kouluttaja pitää esityksen eS 3.1 Sosiaalisen median riskit pptx, jossa linjataan nuorten sosiaalisen median käyttöön liittyviä yleisiä kysymyksiä ja riskejä. Näihin kuuluvat mm. seuraavat:

1. verkkomaineen mahdollinen tahriintuminen ja sen seuraukset
2. virtuaalisen kiusaamisen mahdollisuus (anonyymit kolmannen osapuolen sovellukset, pelit, joissa arvioidaan toisia, gallupit jne.)
3. liiallinen henkilökohtaisten tietojen jakaminen, mikä tekee yksilöstä haavoittuvan
4. identiteettivarkaudet ja petokset
5. yksityisyyden puute sosiaalisessa mediassa – erityisesti salasanojen ja turvallisuuden suhteen
6. "ystävien" tapaaminen kasvotusten
7. linkit sopimattomille sivuille ja sisältöön (mukaan lukien pornosivut ja aikuisille tarkoitettu sisältö)
8. digitaitojen puute yksityisyys- ja turvallisuusasetusten säätämisessä.

Videot, keskusteluaiheet ja käytännön ryhmätyöt on sisällytetty esitykseen.

Huom.: Kouluttajan tulee käsitellä sopimattoman/vaarallisen käytön ja laittoman käytön eroa. Laittoman käytön tapauksessa koulun rehtorin tulee käsitellä asia ja siitä tulee tehdä ilmoitus poliisille. Koulun ohjeistuksessa tulee tehdä ero näiden kahden välillä ja ohjeistaa, kuinka nämä väärinkäyttötyypit käsitellään.

Keskustelua: Monet koulut ja opetusministeriöt käyttävät Internetin sisällönsuodatusta, ja Yhdysvalloissa se on lakisääteistä (Children's Internet Protection Act). Sen seurauksena Facebook, YouTube ja vastaavat sivustot voivat olla estettyinä kouluissa. Mitä etuja ja haittoja sivustojen estämisellä on?

- **@ Dia 16**
  Kouluttaja klikkaa kohtaa "I have read", josta käynnistyy Richard Dreyfussin dramatisoitu luenta Applen käyttöehdoista tai loppukäyttäjän lisenssisopimuksesta. Noin minuutti riittää vitsin tajuamiseen.
- **@ Dia 21**
  Kouluttaja klikkaa "Help"-kuvaa, josta käynnistyy Googlen video Manage your online reputation (Hallitse verkkomainettasi).
- **@ Dia 23**
  Kouluttaja klikkaa linkkiä "social media", josta käynnistyy kolmen minuutin humoristinen video sosiaalisessa mediassa suositeltavista ja vältettävistä teoista, jotka pätevät myös luokkahuoneessa. Lyhennä, jos se on mielestäsi liian pitkä.

- **@Dia 24**
  Kouluttaja kysyy, käyttääkö kukaan eTwinningiä, Edmodoa tai vastaavaa palvelua. Kouluttaja esittelee molemmat palvelut lyhyesti ja pyytää osallistujia jakamaan muutamia hyviä esimerkkejä sosiaalisen median käytöstä opetuksen ja oppimisen tukena.

  Tehtävä: Ryhmä jaetaan kahtia sen mukaan, onko osallistujilla Twitter-tili vai ei.

  Käytännön harjoitus ryhmätyönä: Twitterin käyttäminen.

  Ryhmä 1. Kouluttaja auttaa opettajia luomaan Twitter-tilin ja seuraamaan edu#-kanavia, jotka tukevat jatkuvaa ammatillista kehitystä, esim. edchat tai edchatie.
  Tehtävät:
  Twitter-tilin perustaminen (tähän tarvitaan sähköpostiosoite) - Edu-kanavan seuraaminen - Twiitin lähettäminen ryhmän kanavalle - Twitterin oman turvallisuusoppaan tutkiminen sekä tutustuminen materiaaleihin eS 3.1b 60 tapaa käyttää Twitteriä luokkaympäristössä www.teachthought.com/social-media/60-ways-to-use-twitter-in-the-classroom-by-category/ sekä www.squidoo.com/twittersafetytips

  Ryhmä 2. Jo Twitteriä käyttävien tehtävänä on tutkia Facebookin turvallisuusominaisuuksia ja luoda lyhyt, koulussa opettajille järjestettävä työpaja käyttämällä pohjaa eS 3.1c Opettajien työpajan pohja. Esityksen otsikkona on: "Kuinka käyttää Facebookia turvallisemmin". Seuraavat linkit voivat olla hyödyllisiä:

  - **Facebookin tietoturvaopas :** www.facebook.com/safety/attachment/Guide%20to%20Facebook%20Security.pdf
  - www.fbparents.org Tarkoitettu vanhemmille, mutta siitä saa hyvän yleiskuvan palvelusta.
  - http://facebookforeducators.org/wp-content/uploads/2011/05/Facebook-Edu-Guide.pdf

  Kun osallistujat ovat saaneet workshop-suunnitelman valmiiksi, he voivat lukea seuraavat materiaalit: www.squidoo.com/twittersafetytips tai eS 3.1b 60 tapaa käyttää Twitteriä luokkaympäristössä, 60 tapaa käyttää Twitteriä luokkaympäristössä kategorioittain , www.teachthought.com/social-media/60-ways-to-use-twitter-in-the-classroom-by-category/ ja twiitata niistä.

  Palaute
  Ryhmä kaksi jakaa Twitterissä workshop-ideansa turvallisemmasta Facebookin käytöstä ryhmän yksi kanssa. Ideat laitetaan myös oppimisblogiin.

  Koko ryhmä keskustelee siitä, kuinka koulun sisäisiä henkilöstön työpajoja voidaan käyttää digitaalisen turvallisuuden taitojen ja tietoisuuden

	lisäämiseen. Kouluttaja kehottaa osallistujia jakamaan omia Twitter-kokemuksiaan ja huolenaiheitaan sekä hyviä tapoja käyttää sosiaalista mediaa (kuten Twitteriä) opetuksen tukena. Vaihtoehtoisia työpajaehdotuksia **paikallisiin oloihin muokattua kurssia varten**: • Ryhmä 2 voi keskustella työpajan mukauttamisesta siten, että oppilaat voivat vetää työpajan nuoremmille oppilaille *tai* vanhemmilleen Internet-turvallisuuden teemapäivänä *tai* • He voivat käyttää erilaisia sosiaalisen median työkaluja, esim. Safer Google+:aa tai paikallista verkkoyhteisöpalvelua *tai* • He voivat tehdä tietosivun Instagramin, YouTuben tai Tumblrin tietoturvaominaisuuksista.
Kahvitauko	**15 min**
Tehtävä 3.2:	**Mobiililaitteiden vastuullisen käytön opettaminen ja pedagogisten materiaalien kerääminen**
Kesto	35 min
Tavoitteet	• Tutustua syvällisemmin mobiili- ja sosiaalisen median palveluihin ja jakaa kokemuksia. • Pohtia, kuinka sosiaalisen median palvelujen avulla voi tukea oppimista luokkaympäristössä ja sen ulkopuolella. • Ymmärtää, kuinka luoda ja kehittää vastuullisen käytön säännöt yhdessä oppilaiden kanssa. • Hyödyntää kouluille tarkoitettua Learning Resource Exchange -portaalia ja sen laajaa pedagogisten materiaalien valikoimaa.
Kuvaus	On olemassa opetus- ja oppimismateriaaleja, jotka esittelevät digitaalisen median ja mobiililaitteiden hyödyntämistä luokkaympäristössä. **Materiaalit** Kouluttaja esittelee lyhyesti Learning Resource Exchange -portaalin ja Insafe-osion, jos ei ole tehnyt sitä aiemmin, ja erityisesti aineiston eS 3. 2 Matkapuhelimen käyttäminen koulussa - http://lreforschools.eun.org/web/guest/resource-details?resourceId=407595 Kouluttaja kertoo osallistujille, että he tarkastelevat ryhmissä opettajien ja oppilaiden sosiaalisen median ja mobiililaitteiden käyttöä 35 minuutin ajan. Sen jälkeen pidetään Teachmeet-tyylinen istunto, jossa jokainen ryhmä esittelee *lyhyesti ja suullisesti* (ei PowerPoint-esityksiä) jonkun materiaalin, työkalun tai käytännön ja kertoo, kuinka he hyödyntäisivät sitä opetuksessa. Ryhmä voi myös pitää esityksen siitä, kuinka oppilaille voi opettaa vastuullisen käytön sääntöjä. Kouluttaja jakaa osallistujille mahdollisuuksien mukaan paperikopion Insafe-opetusmateriaalista (materiaali eS 3.2 Matkapuhelimen käyttäminen koulussa).

	Materiaali on saatavilla myös osoitteessa http://lreforschools.eun.org/web/guest/resource-details?resourceId=407595 . Se auttaa osallistujia näkemään, kuinka he voivat muokata vanhoja tuntisuunnitelmiaan tai keksiä omia ideoita tekniikan oppimiskäyttöön. **Huom.:** Kouluttaja nostaa esille sivulla 50 olevan esimerkin 5, joka esittelee erittäin selkeän tavan osallistaa oppilaat ja heidän vanhempansa mobiililaitteiden ja sosiaalisen median vastuulliseen käyttämiseen. **Ryhmätyö** **Tehtävä 1)** Osallistujat jakautuvat pienryhmiin (2 - 3 osallistujaa kussakin ryhmässä) joko mielenkiinnon kohteidensa, työtehtävänsä, oppilaiden iän jne. mukaan. Jokainen ryhmä valitsee jonkun materiaalin muokattavaksi tai luokassa käytettäväksi. Jokainen ryhmä keskustelee ja vaihtaa ideoita sekä tekee luettelon siitä, miten näitä ja muita hyviä materiaaleja voi käyttää oppitunneilla. **Tehtävä 2)** 15 minuutin kuluttua kouluttaja jakaa paperikopion materiaalista eS 3.2a Esimerkki mobiililaitteiden käyttösäännöistä. Materiaalin voi ladata myös verkosta osoitteesta: http://mterin.vic.edu.au/parents/our-policies Ryhmät keskustelevat australialaiskoulun mobiililaiteohjeistuksen pohjalta, kuinka oppilaat, koulu ja opettajat voivat suojautua mahdollisilta riskeiltä, jotka liittyvät mobiililaitteiden ja oman teknologian käyttöön. Mahdollisia keskustelunaiheita ovat: • Osallistujien oman koulun sosiaalisen median ohjeistus (jos sellainen on). • Onko australialaisten ohjeiden kieli helposti ymmärrettävää oppilaille? • Voisiko ohjeita lyhentää, onko kolme sivua liikaa? • Voisiko ohjeita yksinkertaistaa ja muokata oppilaita varten? • Kuinka opettaa oppilaille heidän velvollisuutensa sosiaalisen median ja mobiililaitteiden käytössä koulussa? Kouluttaja muistuttaa osallistujia sivulla 50 olevasta esimerkistä 5, joka esittelee erittäin selkeän tavan osallistaa oppilaat ja heidän vanhempansa mobiililaitteiden ja sosiaalisen median vastuulliseen käyttämiseen. Sen lisäksi kouluttaja muistuttaa ryhmää, että oman teknologian käyttöä käsitellään enemmän moduuleissa 9 ja 10.
Tehtävä 3.3:	**Materiaalien esittely – Teachmeet-menetelmä**
Kesto	30 min
Tavoitteet	Jakaa pedagogisia ideoita ja havaintoja digitaalisesta turvallisuudesta muiden kanssa.
Kuvaus	Jokainen ryhmä esittelee *lyhyesti ja suullisesti* (ei PowerPoint-esityksiä) materiaalin, työkalun tai käytännön ja kertoo, kuinka he hyödyntäisivät sitä opetuksessa. Kun jokainen ryhmä on esiintynyt, kouluttaja aloittaa keskustelun osallistujien keskeisimmistä huolenaiheista, yhtäläisyyksistä ja eroista. Keskustelkaa digitaaliseen turvallisuuteen liittyvistä kysymyksistä, jotka opettajat kokevat tärkeiksi. Kouluttaja

	antaa osallistujien ehdottaa keinoja vähentää näitä riskejä.
Lounas	1 h

Moduuli 3: KURSSIN TUKIMATERIAALIT

Kurssi/Moduuli/Tehtävä	**Kurssin tukimateriaalit**
eS 3.1	Sosiaalinen media – riskit (pptx)
eS 3.1b	60 tapaa käyttää Twitteriä luokkaympäristössä (pdf)
eS 3.1e	Workshop opettajille -pohja (doc)
eS 3.2	Matkapuhelimen käyttäminen koulussa (Käsikirja, jos saatavilla)
eS 3.2a	Esimerkki mobiililaitteiden käyttösäännöistä (pdf) [moniste]
Tukimateriaalia	Nämä aineistot voi lisätä kurssin oppimisalustalle:
eS 3.1c	Twitter-opas vanhemmille ja oppilaille (pdf)
eS 3.1d	Twitter-opas huolestuneille opettajille (pdf)
eS 3.1f	Google Plus ja ammatillisen identiteetin suojaaminen (pdf)
eS 3.1a	Tiedotteita sosiaalisen median tutkimuksesta (pdf)

Kouluttajan käsikirja ja tukimateriaalit

Kurssi:

Digitaalinen turvallisuus: TURVALLISEMPI KOULU JA LUOKKAYMPÄRISTÖ

Moduuli 4:

Digitaalisen turvallisuuden johtaminen: henkilökohtainen turvallisuus ja hyvinvointi

(eS 4.0)

eS 4.0: HENKILÖKOHTAINEN TURVALLISUUS JA HYVINVOINTI

CPDLab-kurssi	**Digitaalinen turvallisuus: Digitaalisen turvallisuuden parantaminen kouluissa**
Moduulin numero	**eS 4.0**
Moduulin nimi	**Digitaalisen turvallisuuden johtaminen: henkilökohtainen turvallisuus ja hyvinvointi**
Vaatimukset moduulin suorittamiseen	• Osallistujilla tulee olla perustaidot tieto- ja viestintätekniikan käytössä sekä kiinnostus digitaalisen teknologian ja Internetin käyttöön opetuksessa ja oppimisessa. • Heillä tulee olla jonkinlainen tuntemus sosiaalisen median palveluista, niiden toiminnasta ja käytöstä. Ihanteellista olisi, jos osallistujat ovat suorittaneet moduulit 1, 2 ja 3. • Osallistujilla tulisi olla moduulin 1 aikana perustettu tili sosiaalisessa kirjanmerkkipalvelussa sekä pääsy oppimisblogiin ja kurssin tukimateriaaleihin.
Kesto	3 tuntia
Kurssipaikka ja moduulin rakenne	• Tämä moduuli järjestetään lähiopetuksena. • Osallistujat työskentelevät pienryhmissä ja käyttävät tulosten esittämiseen tietokoneita ja muita laitteita, kuten kosketustaulua. • Moduuli sisältää käytännön tehtäviä, keskustelua ja ryhmätöitä. • Osallistujia rohkaistaan jatkuvasti etsimään ja valikoimaan materiaaleja ja linkkejä omalla äidinkielellään.
Tarvittavat tilat ja tilajärjestelyt	• Kouluttaja tarvitsee käyttöönsä interaktiivisen valkotaulun, tietokoneen ja langattoman verkon. • Jokainen osallistuja tarvitsee käyttöönsä tietokoneen, jossa on Internet-yhteys. • Tiloissa tulisi olla tarpeeksi virtapistokkeita kannettaville tietokoneille. • Lisäksi osallistujat tarvitsevat tiloja, joihin hajaantua työskentelemään 3–5 hengen pienryhmissä.
Moduulin yleiskuvaus	Kouluttaja esittelee keskeisimmät riskit, joita nuoret voivat kohdata Internetiä käyttäessään. Tässä keskitytään erityisesti identiteetin suojaamiseen, henkilökohtaiseen turvallisuuteen ja yksityisyyteen kohdistuviin riskeihin. Esitys käsittää videoita ja tapaustutkimuksia, minkä lisäksi kouluttaja havainnollistaa asioita ajankohtaisten, aiheeseen liittyvien uutisten avulla. Näin sisältö pysyy myös ajantasaisena. Osallistujille tulisi jakaa Insafe **Online Safety Resources digipacks 2011 – 2013** -materiaali tai linkki materiaaliin. Esityksen jälkeen tässä ja edellisessä moduulissa opittuja asioita tutkaillaan pienryhmissä. Jokainen ryhmä suunnittelee oppilaille oppimistilanteita, joissa tarkas-

	tellaan erilaisia riskienhallintastrategioita. Jokainen ryhmä esittelee menetelmänsä muille ryhmille.
Moduulin tavoitteet	• tunnistaa keskeiset sosiaaliseen mediaan liittyvät riskit • ymmärtää, kuinka opettaa sosiaalisen median turvallista ja vastuullista käyttöä • löytää menetelmiä oman verkkomaineen hallitsemiseen • jakaa taitoja ja ideoita Internetin ja sosiaalisen median käyttämiseen oppimisprosessin tukena • oppia tunnistamaan eri palveluiden vastuullinen käyttö ja oppia suojaamaan itsensä ja oppilaansa niiden käyttöön liittyviltä riskeiltä.
Taitojen ja osaamisen karttuminen tässä moduulissa	Osallistujat • oppivat tunnistamaan sosiaalisen median ja mobiililaitteiden opetuskäyttöön liittyvät turvallisuusriskit • hallitsemaan henkilökohtaiseen turvallisuuteen liittyviä riskejä sosiaalisessa mediassa • ottamaan käyttöön strategioita ammatillisen identiteettinsä suojaamiseksi • työskentelemään yhteistyössä ja jakamaan tietoa ja taitoja muiden osallistujien kanssa • jakamaan materiaaleja ja opetusmenetelmiä • ottamaan digitaalisen turvallisuuden opetuksen osaksi opetusta.
Tarvittavat materiaalit ja välineet	• Kouluttajan tulee lisätä ryhmän oppimisalustalle kurssin sisällöt, luoda oppimispäiväkirja ja keskustelufoorumi sekä järjestää ryhmälle pääsy näihin. • Insafe Online Safety Resources digipacks 2011 – 2012 -materiaali jokaiselle osallistujalle. • Kouluttajalle tietokone, jossa on Internet-yhteys, ja dataprojektori. • Langaton verkko ja kannettavat tietokoneet osallistujille. • Kosketustaulu tulosten esittämiseen.
Vaatimukset kouluttajalle	• Kouluttajalla tulee olla syvällinen ja monipuolinen tietämys digitaalisesta lukutaidosta, digitaaliseen turvallisuuteen liittyvistä kysymyksistä ja digitaalisen turvallisuuden opetussuunnitelmista. • Kouluttajan tulee tuntea EU:n politiikka, joka tähtää Internetin parantamiseen lasten ja nuorten näkökulmasta, Insafen materiaalit ja palvelut sekä paikallisen Safer Internet Centren materiaalit ja kansainvälinen digitaalisen turvallisuuden opetussuunnitelma. • Kouluttajan tulee tutustua kurssin verkkoalueeseen ja kaikkiin kurssin tukimateriaaleihin, jotka on lueteltu jokaisen moduulin lopussa. Jokainen materiaali on luetteloitu kurssin, moduulin ja tehtävän mukaan, esim. eS 1.1 "Ihmisbingo digikansalaisille" • Kouluttajan tulisi tuntea keskeiset sosiaalisen median palvelut ja työkalut sekä pystyä esittelemään ja käyttämään niitä. • Kouluttajan tulisi käyttää sosiaalista kirjanmerkkipalvelua ja luoda Twitter-kanava kurssia varten. Sen lisäksi hänen tulee ymmärtää keskeiset sosiaalisen median ja mobiilityökalujen käyttöön liittyvät digitaalisen turvalli-

	suuden kysymykset.
Lähdeaineistoja ja materiaaleja koulut-tajille	**Katso kaikki moduulia 3 varten luetellut materiaalit** Katso myös kaikki neuvonta-/vinkkisivustot ja aineistot, jotka on lueteltu materiaa-lissa eS 4.1a Digitaalisen turvallisuuden kysymysten esittely **Verkkoyhteisöpalvelut ja koulut. Hyviä neuvoja**. www.childnet.com/blogsafety/teachers.html **Britannian Safer Internet Centre -keskuksen neuvot opettajille verkkomaineen hallitsemiseen** www.saferinternet.org.uk/advice-and-resources/teachers-and-professionals/professional-reputation **Ammatillisen maineen hallitseminen** www.childnet.com/teachers-and-professionals/for-you-as-a-professional/professional-reputation **Opettajille tarkoitettu, Euroopan komission rahoittama neuvontapuhelin digi-taalisen turvallisuuden kysymyksiä varten Britanniassa** www.saferinternet.org.uk/about/helpline **Sosiaalisen median käytön ohjeistus opettajille Skotlannissa** www.gtcs.org.uk/web/FILES/teacher-regulation/professional-guidance-ecomms-social-media.pdf **Turvallisuustyökaluja luokkahuoneessa ja kotona käytettäväksi** www.google.ie/goodtoknow/familysafety/tools/
Arviointivaihtoehdot	• Osallistujat twiittaavat suosikkiaineistostaan/materiaalistaan. • Osallistujat jakavat julkisesti kirjanmerkityt sivustonsa ja seuraavat koulut-tajan ja ainakin yhden muun osallistujan kirjanmerkkejä.
Moduulin jälkeiset jatkotoimenpiteet	Yhteenkoottuna pedagogiset ideat muodostavat ideapankin, jota osallistujat voi-vat hyödyntää omassa opetuksessaan ja jakaa kollegojensa kanssa koululla.
Vaihtoehtoiset tavat toteuttaa moduuli	Ei vaihtoehtoisia toteuttamistapoja.
Toteutus	Tämä moduuli voidaan toteuttaa kansallisella/paikallisella tasolla. Moduulia voidaan mukauttaa rehtoreille ja päätöksentekijöille sopivaksi. Tässä tapauksessa he voivat opetusmateriaalien vertailun sijaan vertailla ja muokata sosiaalisen median ohjeistuksia tai mobiililaitekäytäntöjä tehtävässä 4.2.
Tehtävä 4.1:	**Verkkomaineeseen ja yksityisyyteen liittyviä digitaalisen turvallisuuden kysy-myksiä**
Kesto	1 tunti

Tavoitteet	• Ymmärtää joitain verkkomaineeseen ja yksityisyyteen liittyviä haasteita. • Tutkia olemassa olevia, verkkomainetta ja yksityisyyttä käsitteleviä opetusmateriaaleja. • Pohtia, kuinka verkkomainetta voi hallita.
Kuvaus	Kouluttaja esittelee materiaaleja ja työkaluja, jotka auttavat tiedostamaan ja hallitsemaan erilaisia digitaaliseen turvallisuuteen ja sosiaalisen median käyttöön liittyviä kysymyksiä. Aihetta käsitellään esimerkkien, tapaustutkimusten ja videoiden avulla. Oheinen PowerPoint-esitys eS 4.1 Digitaalisen turvallisuuden kysymyksiin puuttuminen pptx sisältää videoita, linkkejä, tapaustutkimuksia ja työkaluja, jotka havainnollistavat tarjolla olevia erilaisia materiaaleja turvallisen ja vastuullisen sosiaalisen median ja verkkoyhteisöjen käytön opettamiseen. Kaikki videot ja aineistot on linkitetty esityksen kuviin. Yksityiskohtaisia tietoja on diojen muistiinpanoissa. Kouluttaja voi valita näistä tai lisätä esitykseen harkintansa mukaan muita linkkejä. Esitys sisältää myös Googlen Good to Know -kampanjan neuvoja verkkomaineen hallintaan. Kaikki linkit ovat materiaalissa eS 4.1a Digitaalisen turvallisuuden kysymysten esittely. Niitä voidaan hyödyntää tämän tehtävän aikana muun muassa seuraavien aiheiden käsittelyssä: • turvalliset salasanat • yksityisyys ja henkilökohtaisten tietojen ja identiteetin suojaaminen verkossa • henkilökohtainen turvallisuus ja hyvinvointi • vahingolliset kontaktit (esimerkiksi vieraiden ihmisten tapaaminen, joihin on tutustunut verkossa) • vahingollinen sisältö (esimerkiksi materiaali, joka sisältää rotuvihaa, väkivaltaa, itsensävahingoittamista ja pornografiaa) • verkkomaine (henkilökohtainen ja ammatillinen maine). **Tehtävä** Kouluttaja voi antaa osallistujille pääsyn seuraavaan materiaaliin: eS 4.1b Neuvoja opettajille – ammatillisia neuvoja sosiaalisesta mediasta (pdf). Osallistujat voivat lukea materiaalin ja tallentaa sen muistitikuilleen tai pilvipalvelutililleen.
Tehtävä 4.2:	**Käytännön ryhmätehtävä – ideoiden kerääminen oppitunteja varten**
Kesto	1 tunti
Tavoitteet	• Tarkastella olemassa olevia digitaalisen turvallisuuden opetuksen tuntisuunnitelmia.

	• Pohtia, kuinka opettaa digitaalisen jalanjäljen, yksityisyyden ja maineen hallintaa verkossa. • Jakaa tietoa ja käsityksiä pienryhmissä.
Kuvaus	Tässä vaiheessa osallistujilla on jonkinlainen ymmärrys sosiaalisen median käyttöön liittyvistä riskeistä. Kouluttaja antaa heille vähän aikaa tutkia saatavilla olevia aineistoja ja työkaluja, joiden avulla näihin riskeihin voidaan puuttua. Lisäksi osallistujat pohtivat, kuinka näitä aineistoja ja työkaluja voisi käyttää oppitunneilla. • **@ Dia 11 Ryhmätyö** Osallistujat muodostavat pienryhmiä joko mielenkiinnon kohteiden tai opetettavien aineiden perusteella. Ensin he tutustuvat materiaaleihin, valitsevat riskin ja tekevät tuntisuunnitelmat. Sitten he keskustelevat, kuinka he käyttäisivät niitä opetuksessa. Sen jälkeen osallistujat valmistautuvat esittämään ideansa lyhyesti muille yhteisessä istunnossa (4.3) ja kirjaavat tuntisuunnitelmansa Google Doc- tai Etherpad-alustaa käyttämällä http://etherpad.opensourcebridge.org -sivustolla, jonka voi jakaa ryhmän blogissa. Osallistujat kertovat, miksi he valitsivat aiheensa, mitä sosiaalisen median riskejä he käsittelevät ja miksi he valitsivat tietyt materiaalit/työkalut. Lisäksi he selittävät lyhyesti, kuinka opettaisivat valitsemansa aiheen. • Kouluttaja antaa osallistujille oikeudet materiaaliin eS 4.1a Digitaalisen turvallisuuden kysymysten esittely. • Kouluttaja jakaa Insafe Online Safety Resources digipacks 2010–2012 -materiaalin jokaiselle osallistujalle. • Kouluttaja rohkaisee osallistujia käyttämään oman Safer Internet Awareness Centrensä tarjoamia materiaaleja. • Kouluttaja jakaa osallistujien kanssa sosiaalisen kirjanmerkkisivustonsa ja Learning Research Exchange -portaalin osoitteen. http://lreforschools.eun.org/web/guest/insafe • Osallistujat voivat käyttää myös omia sosiaalisia kirjanmerkkitilejään, eTwinning-alustaa sekä tietysti Insafe-sivustoja ja digitaalisen lukutaidon opetussuunnitelmaa, jota tarkasteltiin aiemmassa moduulissa.
Kahvitauko	**15 min**
Tehtävä 4.3:	**Ideoiden jakaminen sosiaalisen median opetusta varten – Teachmeet-menetelmä**
Kesto	45 min
Tavoitteet	Jakaa osallistujien kesken hyviä pedagogisia ideoita sosiaalisen median riskeihin puuttumiseen. Perustaa ideapankki digitaalisen turvallisuuden opetus- ja oppimisideoita varten.
Kuvaus	• Jokainen ryhmä kertoo *lyhyesti* omat opetusideansa muille ryhmille. • Osallistujat kertovat, miksi valitsivat aiheensa, mitä sosiaalisen median ris-

	kejä he käsittelevät ja miksi he valitsivat tietyt materiaalit/työkalut. • Lisäksi he selittävät, kuinka opettaisivat materiaalin. Kouluttaja johtaa keskustelua koko ryhmän kesken ja kokoaa pääkohdat oppimispäiväkirjaan tai muualle.
Tehtävä 4.4:	**Oppimispäiväkirja – pohdintaa**
Kesto	15 min
Tavoitteet	• Tehdä yhteenveto osallistujien päivän aikana oppimista asioista ja siitä, miten he aikovat ryhtyä soveltamaan opittua käytäntöön kouluissaan. • Saada osallistujilta palautetta loppukurssista.
Kuvaus	Osallistujien itsearviointi oppimispäiväkirjaan. Mitä olen oppinut tänään? Mitä tietoa jaan kollegoilleni koululla? Osallistujat voivat sisällyttää oppimispäiväkirjaan myös mahdollisia kommentteja tukimateriaalista eS 4.1b. Osaavatko he nimetä omasta maastaan tahoja, joilta voi saada tukea ongelmatapausten sattuessa? Tässä vaiheessa olisi hyödyllistä saada osallistujilta palautetta käsitellyistä asioista, samoin kuin seuraavan kolmen päivän ohjelmasta. Kurssin kouluttajan tulisi olla valmis mukauttamaan kurssin sisältöä kohtuullisissa määrin osallistujien tarpeiden mukaan.

MODUULI 4: KURSSIN TUKIMATERIAALIT

Kurssi/Moduuli/Tehtävä	Kurssin tukimateriaalit
eS 4.1	Digitaalisen turvallisuuden kysymyksiin puuttuminen (pptx)
eS 4.1a	Digitaalisen turvallisuuden kysymysten esittely (pdf)
eS 4.1b	Ohjeita opettajille – ammatillisia neuvoja sosiaalisen median käyttöön (pdf)

Kouluttajan käsikirja ja tukimateriaalit

Kurssi:

Digitaalinen turvallisuus: TURVALLISEMPI KOULU JA LUOKKAYMPÄRISTÖ

Moduuli 5: Digitaalinen turvallisuus ja asianmukainen käyttö: digitaalinen lukutaito (eS 5.0)

eS 5.0: Digitaalinen turvallisuus ja asianmukainen käyttö: digitaalinen lukutaito

CPDLab-kurssi	**Digitaalinen turvallisuus: Digitaalisen turvallisuuden parantaminen kouluissa**
Moduulin numero	**eS 5.0**
Moduulin nimi	**Digitaalinen turvallisuus ja asianmukainen käyttö: digitaalinen lukutaito**
Vaatimukset moduulin suorittamiseen	Osallistujilla tulee olla perustaidot tieto- ja viestintätekniikan käytössä ja kiinnostus digitaalisen teknologian ja Internetin käyttöön opetuksessa ja oppimisessa. Jokaisella osallistujalla tulisi olla tili sosiaalisessa kirjanmerkkipalvelussa, mahdollisuuksien mukaan Twitter-tili, sekä pääsy oppimisblogiin ja kurssin tukimateriaaleihin.
Kesto	3 tuntia
Kurssipaikka ja moduulin rakenne	Tämä moduuli järjestetään lähiopetuksena. Osallistujia kehotetaan ottamaan mukaan oma kannettava tietokoneensa, sillä moduulin aikana kokeillaan opetettavia asioita käytännössä. Sen lisäksi moduuliin kuuluu tehtäviä, keskustelua, ryhmätöitä ja pohdintaa. Osallistujia rohkaistaan jatkuvasti etsimään ja valikoimaan materiaaleja ja linkkejä omalla äidinkielellään.
Tarvittavat tilat ja tilajärjestelyt	• Kouluttaja tarvitsee käyttöönsä dataprojektorin, valkokankaan, kaiuttimet ja tietokoneen. Mahdollisuus käyttää kosketustaulua voi olla hyödyksi. • Osallistujat tarvitsevat oman kannettavan tietokoneen. • Tiloissa tulisi olla tarpeeksi virtapistokkeita kannettaville tietokoneille sekä kaikkien käytettävissä oleva langaton verkko. • Lisäksi osallistujat tarvitsevat tiloja, joihin hajaantua työskentelemään pienryhmissä.
Moduulin yleiskuvaus	Kouluttaja lisää ryhmän oppimisalustalle kurssin sisällöt, luo oppimispäiväkirjan ja keskustelufoorumin sekä antaa ryhmälle pääsyoikeudet näihin. Kouluttaja esittää PowerPoint-esitykset eS 5.1 Digitaalinen lukutaito ja eS 5.2. Esitykseen on upotettu ryhmätehtäviä, yksilötehtäviä, videoita, keskustelunaiheita ja tehtäviä. Ne käsittelevät sitä, kuinka oppilaita voidaan auttaa käyttämään Internetiä turvallisesti, eettisesti ja asianmukaisesti ja kehittämään digitaalista lukutaitoaan. Jokaiselle osallistujalle tulisi jakaa Insafe-käsikirja "The Web We Want".

	Ryhmätyö auttaa osallistujia valitsemaan digitaalisen lukutaidon opetusta omalle luokalleen. Jokainen ryhmä esittää opetusmenetelmänsä muille ryhmille. Jokaista osallistujaa rohkaistaan tutustumaan joihinkin tarjolla oleviin työkaluihin ja materiaaleihin ja tallentamaan hyödylliset linkit sosiaaliseen kirjanmerkkipalveluun.
Moduulin tavoitteet	• Tarkastella, kuinka opettajat ja koulut voivat luoda turvallisia oppimisympäristöjä ja suojella oppilaita sekä sisällyttää digitaalinen turvallisuus opetussuunnitelmaan ja kaikkeen koulun toimintaan • Tarjota opettajille jäsentynyt lähestymistapa digitaalisen teknologian turvalliseen ja eettiseen käyttöön tiedon käsittelyssä ja hallinnassa • Kehittää tapoja digitaalisen teknologian eettiseen ja vastuulliseen käyttöön • Ymmärtää, että palvelujen käyttöehtojen merkityksen tarkastelu on tärkeää • Käsitellä tiedon etsintään, jakamiseen ja luomiseen liittyviä kysymyksiä (plagiointi, laiton lataaminen, piratismi, Creative Commons -lisenssit, tiedonlähteiden kriittinen arviointi).
Taitojen ja osaamisen karttuminen tässä moduulissa	Osallistujat oppivat • tarjoamaan oppilaille strategioita tiedonhaun hallitsemiseen, tiedon arvioimiseen ja tieto- ja viestintätekniikan käyttöön eri oppiaineissa • harjoittelemaan kriittistä tietoisuutta tietojen hakemiseen, käyttöön ja hankintaan liittyvistä taidoista, kun käytetään digitaalista teknologiaa • arvioimaan, järjestämään, kokoamaan ja yhdistämään digitaalisen teknologian avulla haettua tietoa • osoittamaan tietoisuutta digitaalisen teknologian vastuullisesta ja eettisestä käytöstä • tukemaan oppilaiden oppimista ja osallisuutta käyttämällä digitaalisia sosiaalisia oppimistyökaluja • jakamaan pedagogisia periaatteita, käytännön esimerkkejä ja ideoita niiden soveltamiseen • kehittämään strategioita digitaalisen lukutaidon opettamiseen.
Tarvittavat välineet ja materiaalit	• Pääsy kurssin tukimateriaaliin verkossa. Jokaiselle osallistujalle oma kappale European Schoolnetin julkaisua "The Web We Want " (2013). Julkaisu on saatavilla myös osoitteessa www.webwewant.eu Monisteet eS 5.1a - eS 5.1b - - eS5.2a eS 5.1c voidaan jakaa monisteena tai kurssin oppimisalustalla. • Kouluttajalle tietokone, jossa on Internet-yhteys, ja dataprojektori. • Kosketustaulu. • Kannettavat tietokoneet osallistujille ja pääsy langattomaan verk-

	koon. • Pääsy moduulin tukimateriaaleihin. • Sosiaalinen kirjanmerkkisivusto digitaalista turvallisuutta käsitteleviä linkkejä ja materiaaleja varten.
Vaatimukset kouluttajalle	Kouluttajalla tulee olla syvällinen ja monipuolinen tietämys digitaalisesta lukutaidosta, digitaaliseen turvallisuuteen liittyvistä kysymyksistä ja digitaalisen turvallisuuden opetussuunnitelmista. Kouluttajan tulee tuntea EU:n politiikka, joka tähtää Internetin parantamiseen lasten ja nuorten näkökulmasta, Insafen materiaalit ja palvelut sekä paikallisen Safer Internet Centren materiaalit ja kansainvälinen digitaalisen turvallisuuden opetussuunnitelma. Kouluttajan tulee tutustua kurssin verkkoalueeseen ja kaikkiin kurssin tukimateriaaleihin, jotka on lueteltu jokaisen moduulin lopussa. Jokainen materiaali on luetteloitu kurssin, moduulin ja tehtävän mukaan, esim. eS 1.1 "Ihmisbingo digikansalaisille" Kouluttajan tulee käyttää sosiaalista kirjanmerkkipalvelua (esim. www.delicious.com tai Diigo www.diigo.com) digitaaliseen turvallisuuteen liittyvien linkkien ja materiaalien tallentamista varten. Kouluttajan tulee myös kannustaa osallistujia luomaan oma käyttäjätili kurssilla käsiteltyjen verkkoaineistojen hallinnoimiseksi.
Lähdeaineistoja ja materiaaleja kouluttajille	**The Web We Want, julkaisija European Schoolnet, 2013** www.webwewant.eu **Kathy Schrockin opas kriittiseen arviointiin** www.schrockguide.net/critical-evaluation.html **Informaatiolukutaidon ja kriittisen ajattelun opettaminen** https://sites.google.com/site/teachinfolit/ **Informaatiolukutaidon opettaminen** www.techlearning.com/web-tours/0048/teaching-information-literacy-tips-and-resources/41213 Hyviä sivustoja lapsille. **UNESCO** Informaatiolukutaito opettajille www.unesco.org/new/en/communication-and-information/resources/publications-and-communication-materials/publications/full-list/media-and-information-literacy-curriculum-for-teachers/ **Insafe** www.saferInternet.org Osittain Euroopan unionilta rahoituksensa saava Insafe on eurooppalainen Safer Internet Centre -verkosto, joka edistää turvallista ja vastuullista Internetin ja mobiililaitteiden käyttöä nuorten kes-

kuudessa. Se tarjoaa laajan valikoiman materiaaleja ja tietolähteitä useilla eri kielillä. Jokaisella jäsenmaalla on oma **Safer Internet Awareness Centre.** On mahdollista hyödyntää myös muiden maiden (esimerkiksi englannin- tai ruotsinkielisiä) Safer Internet Awareness Centre -aineistoja.

Safer Internet Day (SID)
www.saferInternetday.org Helmikuun toisena tiistaina vietetään kouluissa vuosittain kansainvälistä Internet-turvallisuuden teemapäivää (Safer Internet Day). EU:n hanke tarjoaa materiaaleja, oppituntisuunnitelmia ja teemapaketteja opettajille ja kouluille.

Teach today
www.teachtoday.eu/ Teachtoday-sivusto tarjoaa opettajille, rehtoreille ja muille koulujen työntekijöille tietoa ja neuvoja uuden tekniikan myönteiseen, vastuulliseen ja turvalliseen hyödyntämiseen.

Digitaalinen osaaminen ja digitaalinen lukutaito
http://linked.eun.org/web/guest/policyMaker Osittain Euroopan komission rahoittama projekti, joka tarkastelee tieto- ja viestintätekniikkaa hyödyntävän, innovatiivisen opetuksen ja oppimisen tutkimusta, politiikkaa ja käytäntöjä.

Kaikki alla listatut materiaalit ja muita materiaaleja löytyy osallistujien asiakirjasta (Participant document): eS 5.2c Opetusmateriaaleja – kriittinen ajattelu ja eettinen käyttö.

Tekijänoikeudet
Copyrightkids**:** www.copyrightkids.org
Cyberbee Copyright interactive**:** www.cyberbee.com/cb_copyright.swf
Tekijänoikeudet: www.teachingcopyright.org
Childnetin tekijänoikeuksien työkalupakki: www.childnet.com/kia/toolkit UK

Creative Commons
Creative Commons -lisenssit: http://creativecommons.org/
Creative Commons lapsille: www.youtube.com/watch?v=YtJdfHXk_u8
Common Craft – tekijänoikeudet ja Creative Commons -lisenssit: www.commoncraft.com/video/copyright-and-creative-commons

CC-lisensoidut kuvat ja media oppilaiden käyttöön
http://commons.wikimedia.org/wiki/Main_Page

Lainaukset
Mitä se tarkoittaa? Kuinka lainata oikein? http://plagiarism.org/citing-sources/overview/

Työkalu www.bibme.com **tai** www.easybib.com

	Plagiointi www.plagiarism.org **Ohjeita opettajille** www2.ofqual.gov.uk/files/2009-12-24-plagiarism-teachers.pdf **Ohjeita vanhemmille** www2.ofqual.gov.uk/files/2009-12-24-plagiarism-parents.pdf **Ohjeita oppilaille** www2.ofqual.gov.uk/files/2009-12-24-plagiarism-students.pdf **Materiaalit** www.plagiarismadvice.org
Arviointivaihtoehdot	• Jokainen osallistuja twiittaa ryhmän Twitter-kanavalle jotain kriittiseen ajatteluun ja digitaaliseen lukutaitoon liittyvää. • Osallistujat tallentavat hyödyllisiä linkkejä ja verkko-osoitteita sosiaaliselle kirjanmerkkitililleen.
Moduulin jälkeiset jatkotoimenpiteet	Ei ole.
Vaihtoehtoiset tavat toteuttaa moduuli	Ei vaihtoehtoisia toteuttamistapoja.
Toteuttamisvaihtoehdot kansallisella/paikallisella tasolla	Tämä moduuli voidaan toteuttaa kansallisella/paikallisella tasolla. Tämä moduuli on hyödyllisin opettajille ja heidän oppilailleen. Osallistujat voivat olla eri aineiden opettajia ja eri kouluista.
Tehtävä 5.1:	**Asianmukaisen käytön opettaminen**
Kesto	1 h 15 min
Tavoitteet	• Ymmärtää termien 'digitaalinen lukutaito', 'kriittinen ajattelu' ja 'eettinen käyttö' merkitys. • Ymmärtää, että oppilaille täytyy opettaa digitaalista osaamista. • Työskennellä yhteistyössä ryhmänä • Tarkastella erilaisia opetustyökaluja ja -materiaaleja • Jakaa materiaaleja, työkaluja ja menetelmiä digitaalisten mediataitojen ja osaamisen opettamiseksi.
Kuvaus	Kouluttaja käyttää PowerPoint-esitystä eS 5.1 Digitaalinen lukutaito (pptx). Diojen muistiinpanoissa on lisää muistiinpanoja. • **@ Dia 2** Kouluttaja napsauttaa kuvaa -**linkitetty videoon**: Sosiaalinen

media koulutuksessa – Diginatiivien opettaminen vuonna 2011: https://www.youtube.com/watch?v=3zKdPOHhNfY&feature

=endscreen&NR=1

Kouluttaja valitsee näkyville seuraavan kysymyksen:
"Teknologia on tärkeää, mutta kuinka opettaa heille lukutaitoa?"

Ennen aikaan oppikirjalla oli valta-asema. Kirjat toimitettiin, tiedot varmennettiin, tarkistettiin ja vahvistettiin, ja kirjojen kirjoittajat olivat alallaan arvostettuja. Ennen julkaisua kirjat testattiin ja arvioitiin luokkaympäristössä. Nykyisin oppilaiden käytössä on Internet ja Wikipedia. Omasta mielestään he saattavat olla hyviä tiedonhaussa, koska he osaavat käyttää Googlea tai Wikipediaa, mutta pitääkö tämä paikkansa? Osaavatko oppilaat hakea tietoa turvallisesti ja eettisesti? Osaavatko he arvioida ja valita hyödyllisiä blogeja, videoita tai muita tietolähteitä verkossa?

- **@ Dia 4**
  Näihin **tehtäviin** käytetään aikaa max. 10 min. **Jokainen osallistuja hakee tietoja verkosta**.

  Tehtävä 1
  Kaikki osallistujat menevät hakusivustolle ja tekevät haun: Hoax Websites (huijaussivustot). Kouluttaja kysyy:

  Kuinka kauan hakutulosten saaminen kesti?
  Kuinka monta miljoonaa hakutulosta saitte?
  Miksi niitä on niin paljon?
  Luuletko, että oppilaasi tunnistaisivat olevansa huijaussivustolla?

  Tehtävä 2
  Osallistujat jakautuvat nyt kahteen ryhmään. Toinen ryhmä tekee haun ”itsemurha”' ja toinen haun ”kuinka rakentaa pommi”, minkä jälkeen ryhmät jakavat tulokset toisilleen.
  Sama toistetaan hauilla ”anoreksia” ja ”itsensä vahingoittaminen”.
  Mitä reaktioita ja kommentteja ne herättävät osallistujissa?
  [Jotkut ryhmäläiset eivät välttämättä halua tehdä hakua kaikilla näillä termeillä.]

  Tehtävä 3
  Koko ryhmä tekee haun: Martin Luther King. Kouluttaja etsii hakutuloksista sivuston www.martinlutherking.org ja kiinnittää ryhmän huomion siihen, monentenako hakutuloksena sivusto on. Monennellako sivulla se on hakutuloksissa? (Kouluttajan tulisi selittää, että Googlen oman tutkimuksen mukaan ihmiset selaavat tuloksia harvoin ensimmäistä hakutulossivua pidemmälle, iästä riippumatta. Kouluttaja pyytää ryhmää nyt avaamaan sivuston www.martinlutherking.org ja selvittämään, kuka on sivuston tekijä/omistaja. Mitä se kertoo sivustosta? Jos osallistujat eivät tiedä, kouluttaja tekee haun ”Stormfront”.

(Sivusto on rotuvihasivusto. Sisällönsuodatuksen vuoksi sille ei luultavasti pääse useimmissa kouluissa, mutta kuten todettiin, se on helposti saatavilla koulujen ulkopuolella.)

Keskustelua: Mitä voimme tehdä? Sisällönsuodatus on hyödyllistä, mutta sillä on rajoituksensa. Mitä taitoja ja strategioita oppilaille tulisi opettaa? Digitaalista lukutaitoa, vahvuutta, joustavuutta ja selviytymiskeinoja?

- **@ Dia 7**
  Ryhmätehtävä 1 Kesto max. 10 min.
  Osallistujat työskentelevät ryhmissä monisteen 1 avulla:
  Kouluttaja jakaa osallistujat 4–5 hengen pienryhmiin. Moniste eS 5.1a Digitaalisen ajan lukutaidot – Tiedonhaku. Lyhyt suullinen palaute koko ryhmälle ryhmätehtävästä.

- **@ Dia 9**
  Ryhmätehtävä 2: Osallistujat jakautuvat kahteen ryhmään ja työskentelevät monisteen 2 avulla: Kouluttaja jakaa osallistujat 4–5 hengen pienryhmiin. Max. 10 min.
  Moniste eS 5.1b Digitaalisen ajan lukutaidot – Kriittinen ajattelu.
  Lyhyt suullinen palaute koko ryhmälle ryhmätehtävästä.

  HUOM.: Neljäs taito käsitellään seuraavassa tehtävässä.

- **@ Dia 11**
  Tehtävä osallistujille 10 - 15 min Kouluttaja jakaa osallistujille seuraavan materiaalin tai antaa heille pääsyn siihen: eS 5.1c Opetusmateriaaleja – kriittinen ajattelu ja eettinen käyttö. **Tehtävä:** Kouluttaja pyytää osallistujia tutustumaan eri työkaluihin, esim. Easybib, Plagiarism.org ja Imagecodr, ja kirjoittamaan lyhyen kuvauksen hyödyllisiksi kokemistaan työkaluista suoraan eS 5.2c -asiakirjaan.

- **@Dia 12**
  Kouluttaja voi esitellä muutamaa työkalua, joita **ei** ole listattu materiaalissa eS 5.1c Opetusmateriaaleja – kriittinen ajattelu ja eettinen käyttö. Kaikkia diassa listattuja ei ehdi käydä läpi.

- **@ Dia 13**
  Kouluttaja näyttää yhden työkalun ja kysyy osallistujilta, onko joukossa heille uusia työkaluja ja mitkä työkalut he haluaisivat nähdä. Kouluttaja näyttää vielä yhden tai kaksi työkalua ja kysyy sitten, onko kellään ryhmässä ehdotuksia työkaluksi, jota heidän oppilaansa haluaisivat käyttää.

- **@Dia 14**
  eSafety Label -työkalua tarkastellaan tarkemmin moduulissa 9. Sitä voidaan hyödyntää koko koulun digitaalisen turvallisuuden toimintasuunnitelman luomisessa.

- **@ Dia 15**
  Kouluttaja muistuttaa osallistujia myös monista materiaaleista, jotka ovat saatavilla Insafe- ja Learning Resource Exchange -portaaleissa.

	• **@ Dia 18** Kouluttaja käynnistää infografiikkaa napsauttamalla Ted Koppelin videon informaatioylikuormituksesta.
Tehtävä 5.2	**Tietojen julkaiseminen ja välittäminen maailmanlaajuiselle yleisölle**
Kesto	45 min
Tavoitteet	• Kehittää strategioita kunnioittavan verkkokeskustelun ja -kommentoinnin opettamiseksi oppilaille. • Tarkastella tapoja opettaa digitaalista lukutaitoa. • Vaihtaa ajatuksia opetusmetodeista ja -strategioista muiden osallistujien kanssa.
Kuvaus	**Tehtävä 1** Kouluttaja näyttää esityksen eS 5.2 Maailmanlaajuiselle yleisölle kirjoittaminen pptx Aikuiset ovat jättäneet tyhjiön verkkoyhteisöihin. Sitä ei tapahdu oikeassa maailmassa, missä suojelemme lapsia ja nuoria kaikin keinoin. Meidän täytyy ryhdistäytyä, toimia valvojana ja tarjota opastusta kaikissa paikoissa, joissa nuoret viettävät aikaansa – etenkin verkossa. Kouluttaja kysyy ryhmältä, mitä kysymyksiä tai ongelmia asiaan liittyy. **@Dia 7** Ryhmä keskustelee, missä kohdin esimerkin oppilas on tehnyt virheitä. Osaavatko osallistujat nimetä kaikki kohdat, joissa tarvitaan muutoksia? Kouluttaja ehdottaa, että jos oppilaalle olisi näytetty, kuinka profiili luodaan (uusi lukutaitovaatimus 2000-luvulle!), hän ei olisi tehnyt niin paljon virheitä. Kouluttaja kysyy osallistujilta ehdotuksia tällaisten ongelmien välttämiseksi. Kouluttaja ehdottaa ennaltaehkäisyä eli profiilin kirjoittamisen opetusta ja tuntisuunnitelman rakentamista aiheen ympärille. Esimerkiksi oppilaille, jotka ovat vanhempia kuin esimerkkiprofiilin Amy, voi näyttää profiilin ja pyytää heitä parantelemaan sitä. Vanhempia oppilaita voi myös pyytää pitämään nuoremmille workshopin, jossa jaetaan vinkkejä profiilin luomiseen ja käytetään Amyn profiilia esimerkkinä. HUOM.: Kouluttaja selittää lopuksi, että profiili on fiktiivinen, mutta kuva ei, joten kasvot on sumennettu. **Keskustelua** • Oppilaille täytyy opettaa, mikä on heidän vastuunsa, kun he julkaisevat tai levittävät jotain digitaalisessa mediassa. • Heidän täytyy ymmärtää, mitä kunnianloukkaus, kiihotus ja herjaaminen tarkoittavat, ja mitä seurauksia haitallisen materiaalin julkaisulla verkossa on.

Keskustelua

- Vastuullisen kirjoittamisen ja tiedon välittämisen opettaminen. Minkälaista ohjeistusta voimme antaa oppilaille?
- Kuinka parhaita käytäntöjä voi mallintaa kouluissa (käyttämällä verkkotyökaluja, joten oppilaat voivat soveltaa oppimaansa aina kun ovat verkossa)?

Meidän täytyy tarjota oppilaille riskinhallintastrategioita ja kehittää heidän vahvuuttaan ja joustavuuttaan selvitä ongelmista. Digitaalinen teknologia antaa oppilaille mahdollisuuden päästä käsiksi monenlaisiin tietolähteisiin, joita käyttämällä he voivat luoda laadukkaita tuotteita myös laajemmalle yleisölle kuin opettajalleen. Digitaalisten työkalujen avulla oppilaat voivat tehdä yhteistyötä ja luoda, julkaista ja levittää omia digitaalisia tuotteitaan, joilla he osoittavat oppimistaan.

Tehtävä 2
Parityö

- Mitä turvallisuustaitoja oppilaat tarvitsevat?
- Mitä materiaaleja voimme käyttää näiden taitojen opettamiseen/esittelyyn?

Tehtävä a) eS 5.2a Digitaalinen lukutaitovaatimus nro 4 Osallistujat tekevät tehtävän pareittain. (Heidän tulisi pystyä hyödyntämään moduulissa 5.1 tekemäänsä työtä.)
Tehtävä b) Etsi tiedon julkaisua ja välittämistä käsitteleviä materiaaleja (esim. Web We Want, Common Sense Media , YouTube tai muita oman maan Safer Internet Awareness Centren listaamia materiaaleja). Lähetä twiitti, johon liität linkkejä materiaaleihin.

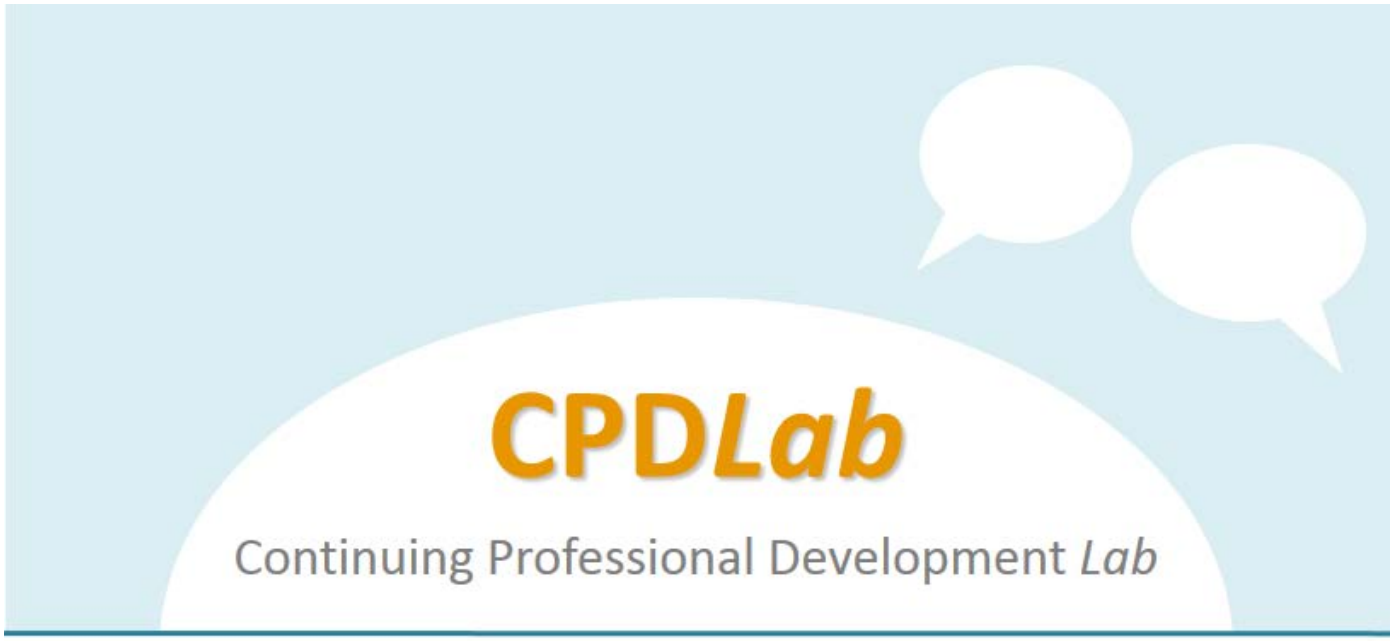
Kahvitauko	15 min
Tehtävä 5.3:	**Digitaalisen lukutaidon opettaminen**
Kesto	1 h
Tavoitteet	• Tutustua hetken aikaa erilaisiin Insafe-verkoston opetus- ja opiskelumateriaaleihin ja pohtia, kuinka niitä voisi hyödyntää koulussa. • Perehtyä syvällisemmin digitaaliseen lukutaitoon ja jakaa kokemuksia siitä. • Pohtia, kuinka kriittistä ajattelua ja digitaalista lukutaitoa voidaan opettaa osana opetettavaa ainetta ja käyttää oppimisen tukena luokkaympäristössä ja sen ulkopuolella. • Jakaa ja vaihtaa pedagogisia käytäntöjä muiden osallistujien kanssa.
Kuvaus	Insafe-opetusmateriaali eS 5.3 The Web We Want (jos mahdollista, jaettavaksi paperikopiona), saatavana myös osoitteessa www.webwewant.eu, auttaa osallistujia näke-

	mään, kuinka olemassa olevia tuntisuunnitelmia voi käyttää tai muokata digitaalisen lukutaidon ja kriittisen ajattelun opettamiseen oppilaille. Kouluttaja kiinnittää osallistujien huomion The Web We Want -käsikirjan lukuun 2 'Information is not knowledge' ja lukuun 6 'The artist in you', jotka käsittelevät kriittistä ajattelua sekä tekijänoikeuksia ja immateriaalioikeuksia. **Ryhmätyö** Osallistujat jakautuvat 3 - 4 hengen pienryhmiin opettamansa aineen, työtehtävänsä, oppilaiden iän jne. mukaan **Tehtävä 1** Lukua 2 käsittelevä ryhmä listaa viisi sääntöä tehokkaaseen tiedonhakuun verkossa ("List 5 rules for looking up information online effectively") ja keskustelee muista luvussa mainituista materiaaleista, joita voisi käyttää luokkaympäristössä. Lukua 6 käsittelevä toinen ryhmä tekee tekijänoikeusvisailun The Web We Want -käsikirjan sivulla 43. Jos ryhmä on suuri, kolmas ryhmä voi tehdä tehtävän aiheesta 'Asian kaksi puolta' ("Two sides of the story") sivulla 46. Keskustelkaa siitä, kuinka ryhmät edistyivät ja olisivatko kyseiset tehtävät hyödyllisiä oppilaille. **Tehtävä 2** Kouluttaja antaa osallistujien käyttöön materiaalin eS 5.1c Opetusmateriaaleja – kriittinen ajattelu ja eettinen käyttö. Jokainen ryhmä tarkastelee materiaaleja ja eS 5.3 The Web We Want -käsikirjan muita lukuja. He vaihtavat ajatuksia siitä, kuinka käsikirjassa ja materiaalissa eS 5.1c esiteltyjä materiaaleja ja menetelmiä voisi käyttää digitaalisen lukutaidon opettamisessa. Osallistujien tulisi pohtia, kuinka he voisivat käyttää materiaaleja luokassa ja tarjota näin oppilaille mahdollisuuksia kehittää digitaalista lukutaitoaan. Valittuaan yksi tai kaksi menetelmää joko materiaaleista eS 5.3 The Web We Want tai eS 5.1c Opetusmateriaaleja – kriittinen ajattelu ja eettinen käyttö osallistujat päättävät, minkä niistä he esittelevät lyhyesti tehtävässä **5.4, Opetus- ja oppimistapojen jakaminen.** Esityksen painopisteen tulisi olla siinä, miten he käyttäisivät materiaaleja luokkaympäristössä.
Tehtävä 5.4	**Opetus- ja oppimistapojen jakaminen – Teachmeet-menetelmä**
Kesto	45 min
Tavoitteet	Jakaa pedagogisia ideoita ja havaintoja digitaalisesta turvallisuudesta muiden kanssa.
Kuvaus	Jokainen ryhmä esittelee *lyhyesti ja suullisesti* yhden materiaalin tai työkalun ja kertoo, kuinka he hyödyntäisivät sitä opetuksessa ja oppimisessa. Jokainen kertoo ryhmälle • opettamansa aineen ja oppilaiden iän • heidän oppituntinsa/opetustehtävänsä otsikon ja aiheen • oppitunnilla käsiteltävän, digitaaliseen turvallisuuteen liittyvän kysymyksen tai työkalun • pääasialliset digitaalisen turvallisuuden materiaalit, joita he hyödynsivät oppitunnin kehittelyssä.

	Kun jokainen ryhmä on esiintynyt, kouluttaja aloittaa keskustelun osallistujien keskeisimmistä huolenaiheista, yhtäläisyyksistä ja eroista. Ryhmä keskustelee digitaaliseen turvallisuuteen liittyvistä kysymyksistä, jotka opettajat kokevat tärkeiksi, ja kouluttaja pyytää osallistujia ehdottamaan keinoja näiden riskien vähentämiseksi.
Lounas	1 h

Moduuli 5: KURSSIN TUKIMATERIAALIT

Kurssi/Moduuli/Tehtävä	Kurssin tukimateriaalit
eS 5.1	Digitaalinen lukutaito (pptx)
eS 5.1a	Digitaalisen ajan lukutaidot – Tiedonhaku (pdf) [moniste]
eS 5.1b	Digitaalisen ajan lukutaidot – Kriittinen ajattelu (pdf) [moniste]
eS 5.1c	Opetusmateriaaleja – kriittinen ajattelu ja eettinen käyttö. (pdf)
eS 5.2	Tietojen julkaiseminen maailmanlaajuiselle yleisölle pptx
eS 5.2a	Digitaalinen lukutaitovaatimus nro 4 (docx) [moniste]
eS 5.3	The Web We Want – käsikirja [monisteena, jos saatavilla]



Kouluttajan käsikirja ja tukimateriaalit

Kurssi:

Digitaalinen turvallisuus: TURVALLISEMPI KOULU JA LUOKKAYMPÄRISTÖ

Moduuli 6: TVT:n epäasialliseen käyttöön puuttuminen

(virtuaalinen kiusaaminen ja seksuaalissävytteinen viestittely)

(eS 6.0)

eS 6.0: TVT:N EPÄASIALLISEEN KÄYTTÖÖN PUUTTUMINEN (VIRTUAALINEN KIUSAAMINEN JA SEKSUAALISSÄVYTTEINEN VIESTITTELY)

CPDLab-kurssi:	Digitaalinen turvallisuus: Digitaalisen turvallisuuden parantaminen kouluissa
Moduulin numero	**eS 6.0**
Moduulin nimi	**TVT:n epäasialliseen käyttöön puuttuminen: virtuaalinen kiusaaminen ja seksuaalissävytteinen viestittely**
Vaatimukset moduulin suorittamiseen	Osallistujilla tulee olla perustaidot Internetin käytössä ja kokemusta sosiaalisen median käyttämisestä. Osallistujien tulisi päästä oppimispäiväkirjaan ja kurssin tukimateriaaleihin, ja heillä tulisi olla käyttäjätili sosiaalisessa kirjanmerkkipalvelussa, jotta he voivat tallentaa ja valikoida materiaaleja moduulin aikana. Tilapäinen sähköpostiosoite sivustoille rekisteröitymistä varten on hyödyksi. Ihanteellista olisi, jos osallistujat ovat suorittaneet moduulit 1 ja 2. Osallistujien tulee suorittaa seuraava moduulin 6 ennakkotehtävä ennen kurssia: • Käsitelläänkö koulusi toimintaohjeissa kiusaamista ja virtuaalista kiusaamista? • Missä toimintaohjeissa näitä ongelmia käsitellään? Kuvaa, kuinka koulussasi käsitellään virtuaaliset kiusaamistapaukset. • Järjestääkö koulusi oppitunteja virtuaalisesta kiusaamisesta tai onko sillä opetusohjelma aiheesta? Kuka pitää oppitunnit tai vetää opetusohjelmaa? • Millaista ohjausta ja tukea on saatavilla paikallisella, alueellisella ja kansallisella tasolla? Millaisia materiaaleja on käytetty onnistuneesti? Laadi digitaalinen luettelo kaikista oppitunneista ja materiaaleista, joiden avulla koulussasi on onnistuneesti puututtu virtuaaliseen kiusaamiseen. Tuo luettelo mukanasi kurssille.
Kesto	3 tuntia
Kurssipaikka ja moduulin rakenne	Tämä moduuli järjestetään lähiopetuksena. Osallistujia kehotetaan ottamaan mukaan oma kannettava tietokoneensa, sillä moduulin aikana kokeillaan opetettavia asioita käytännössä. Sen lisäksi moduuliin kuuluu tehtäviä, keskustelua, ryhmätöitä ja pohdintaa. Osallistujat työskentelevät pienryhmissä. Ennakkomateriaalia käytetään tukena keskustelussa siitä, kuinka koulut voivat puuttua virtuaaliseen kiusaamiseen. Osallistujia rohkaistaan jatkuvasti etsimään ja valikoimaan materiaaleja ja linkkejä omalla äidinkielellään.

Tarvittavat tilat ja tila-järjestelyt	• Kouluttaja tarvitsee käyttöönsä kosketustaulun, tietokoneen ja langattoman verkon. • Jokainen osallistuja tarvitsee käyttöönsä tietokoneen, jossa on Internet-yhteys. • Tiloissa tulisi olla tarpeeksi virtapistokkeita kannettaville tietokoneille. • Osallistujat tarvitsevat tiloja, joihin vetäytyä työskentelemään 3–5 hengen ryhmissä. Sen lisäksi koulutustilassa tulee olla tilaa liikkua tehtävien, kuten esimerkiksi moraalikompassin, aikana.
Moduulin yleiskuvaus	Kouluttaja johtaa keskustelua virtuaalisesta kiusaamisesta ja sen eri muodoista. Osallistujat pohtivat kiusaamisen vaikutuksia ja kiusaamiseen liittyviä rooleja. (Kiusaaja, kiusattu, sivustakatsojat, perheenjäsenet, koulun henkilöstö jne.) Kouluttaja käsittelee kiusatun puolustajan roolia. Painopisteen tulisi olla lasten ja nuorten suojelemisessa ja turvallisen oppimisympäristön luomisessa. Painotus on koko koulun kattaviin toimenpiteisiin liittyvissä strategioissa. Keskustelussa viitataan viimeisimpään virtuaalista kiusaamista koskevaan tutkimustietoon ja siihen, että nuoret eivät välttämättä kerro avoimesti ongelmistaan. Keskustelussa käsitellään virtuaalisen kiusaamisen eri muotoja, mukaan lukien "tahatonta virtuaalista kiusaamista". Osallistujille annetaan työkaluja ja materiaaleja, joiden avulla voi lisätä tietoisuutta ja ratkoa joitain kiusaamiseen liittyviä ongelmia osana koko koulun toimintakulttuuria. Kouluttaja esittelee osallistujille myös käsitteen seksuaalissävytteinen viestittely tai seksiviestittely (sexting) eli seksuaalissävytteisten kuvien ja viestien lähettäminen ja kuinka tämä koskettaa lapsia, nuoria, kouluja, vanhempia ja opettajia. Osallistujille annetaan käyttöön tasokkaita, jo olemassa olevia materiaaleja, joiden avulla asiaan voi puuttua.
Moduulin tavoitteet	• Keskustella virtuaalisesta kiusaamisesta ja sen eri muodoista • jakaa kokemuksia virtuaaliseen kiusaamiseen liittyvistä ongelmista ja sen vaikutuksista kouluissa • Kehittää ja jakaa strategioita, joiden avulla kouluissa voidaan keskustella ja puuttua virtuaaliseen kiusaamiseen jo ennakolta ja oppilaat voivat kertoa virtuaalisista kiusaamistapauksista • Oppia ymmärtämään paremmin Internetin vaikutusta seksuaalisuuteen liittyviin kysymyksiin (seksuaalissävytteinen viestittely, nuorten seksualisointi) • Jakaa tietoa, ideoita, materiaaleja ja työkaluja tietoisuuden lisäämiseksi seksuaalissävytteiseen viestittelyyn liittyvistä kysymyksistä.
Taitojen ja osaamisen karttuminen moduulissa	Osallistujat oppivat • ymmärtämään virtuaalisen kiusaamisen eri muotoja ja eläytymään eri toimijoiden rooliin virtuaalisissa kiusaamistapauksissa • soveltamaan omissa kouluissaan strategioita virtuaaliseen kiusaamiseen puuttumisessa ja virtuaalisesta kiusaamisesta keskusteltaessa • ymmärtämään nuorten kohtaamia seksuaalisuuteen liittyviä haasteita verkossa: seksuaalissävytteinen viestittely, pornografian helppo saatavuus ja nuorten seksualisointi mediassa, sekä internetissä että muualla

	käyttämään ja jakamaan materiaaleja, joiden avulla näihin kysymyksiin voidaan puuttua kouluissa.
Tarvittavat materiaalit ja välineet	• Tunnebarometrikortit tulostettuna. Kortit voi ladata ja tulostaa seuraavan linkin kautta: www.saferInternet.org/web/guest/countdown-gifts • A3-kokoisia papereita World Café -tehtävää varten. • Kompassisuuntien tulosteet Moraalikompassi-tehtävää varten. Ne ovat piilotetuissa dioissa PowerPoint-esityksen eS 6.3 Seksuaalissävytteinen viestittely ja Moraalikompassi lopussa. Sinitarraa. • Kouluttajalle tietokone, jossa on Internet-yhteys, ja dataprojektori. • Kosketustaulu • Kannettavat tietokoneet osallistujille ja pääsy langattomaan verkkoon. • Salasanat kurssisisältöjen verkkoalueelle ja oppimispäiväkirjaan (Kouluttaja luo ennen kurssin alkua kurssille verkko-oppimisympäristön käyttämällä Schoology, Moodlea tai vastaavaa alustaa.)
Vaatimukset kouluttajalle	• Kouluttajan tulee tuntea virtuaalisen kiusaamisen eri muodot, kiusaamisen mekanismit ja kiusaamisen dynamiikka. Erityistä huomiota kiinnitetään kiusaamisen ehkäisyyn kouluissa. • Kouluttajalla tulee olla peruskäsitys siitä, mitä seksuaalissävytteinen viestittely tarkoittaa, ja hänen tulee pystyä antamaan esimerkkejä siitä ja tarjoamaan ryhmälle erilaisia materiaaleja. Seuraavat yhteenvedot voivat auttaa kouluttajaa valmistautumisessa: www.saferInternet.org.uk/sexting ja www.cybersmart.gov.au/tagged/schools.htm • Kouluttajalla tulee olla syvällinen ja monipuolinen tietämys digitaalisesta lukutaidosta, digitaaliseen turvallisuuteen liittyvistä kysymyksistä ja opetussuunnitelmasta. Kouluttajan tulee tuntea EU- politiikka, jonka tavoitteena on tehdä Internetistä turvallisempi lasten ja nuorten näkökulmasta, Insafen materiaalit ja palvelut sekä paikallisen Safer Internet Centren materiaalit ja kansainvälinen digitaalisen turvallisuuden opetussuunnitelma. • Kouluttajan tulee tutustua kurssin verkkoalueeseen ja kaikkiin kurssin tukimateriaaleihin, jotka on lueteltu jokaisen moduulin lopussa. Jokainen materiaali on luetteloitu kurssin, moduulin ja tehtävän mukaan, esim. eS 1.1 "Ihmisbingo digikansalaisille" • Kouluttajan tulee käyttää sosiaalista kirjanmerkkipalvelua (esim. www.delicious.com tai Diigo, www.diigo.com) digitaaliseen turvallisuuteen liittyvien linkkien ja materiaalien tallentamiseksi. Kouluttajan tulee myös kannustaa osallistujia luomaan oma käyttäjätili kurssilla käsiteltyjen verkkoaineistojen hallinnoimiseksi.
Lähdeaineistot ja materiaalit kouluttajalle	**Insafe** www.saferInternet.org Osittain Euroopan unionin rahoittama Insafe on eurooppalainen Safer Internet Centre -verkosto, joka edistää turvallista ja vastuullista Internetin ja mobiililaitteiden käyttöä nuorten keskuudessa. Se tarjoaa laajan valikoiman materiaaleja ja tietolähteitä useilla eri kielillä. Jokaisella jäsenmaalla on oma **Safer Internet**

Awareness Centre
On mahdollista hyödyntää myös muiden maiden (esimerkiksi englannin- tai ruotsinkielisiä) Safer Internet Awareness Centre -aineistoja.

Safer Internet Day (SID)
www.saferInternetday.org Helmikuun toisena tiistaina vietetään kouluissa vuosittain kansainvälistä Internet-turvallisuuden teemapäivää (Safer Internet Day). EU:n hanke tarjoaa materiaaleja, oppituntisuunnitelmia ja teemapaketteja opettajille ja kouluille.

Euroopan komissio
"Eurooppalainen strategia Internetin parantamiseksi lasten näkökulmasta", saatavana useilla eri kielillä:
http://ec.europa.eu/information_society/activities/sip/policy/index_en.htm

Virtuaaliseen kiusaamiseen liittyvät materiaalit

Virtuaalisen kiusaamisenehkäisyn työkalupakki kouluille ja opettajille
http://m.commonsensemedia.org/
educators/cyberbullying-toolkit Common Sense Media:

Virtuaalinen kiusaaminen ja kiusaamisen vastainen työ kouluissa – raportti Safe to learn: Embedding anti-bullying work in school: -
www.digizen.org/downloads/CYBERBULLYING.pdf Department of Children, Schools and Families (Britannia)

Action Plan on Bullying, 2013 Dept of Education and Skills, Irlanti.
www.education.ie/en/Publications/Education-Reports/Action-Plan-On-Bullying-2013.pdf

Digizen www.digizen.org Digizen-sivusto tarjoaa tietoa opettajille, vanhemmille, huoltajille ja nuorille. Sen tarkoituksena on rohkaista teknologian käyttäjiä olemaan vastuullisia digikansalaisia. Sivustolla jaetaan neuvoja ja materiaaleja, jotka käsittelevät esimerkiksi verkkoyhteisöjä ja virtuaalista kiusaamista ja sitä, miten ne liittyvät ja vaikuttavat ihmisten käyttäytymiseen ja kokemuksiin verkossa.

Beatbullying-sivusto
Virtual Violence: protecting children from cyberbullying:
www.beatbullying.org/pdfs/Virtual%20Violence%20%20Protecting%20Children%20from%20Cyberbullying.pdf

Teach today
www.teachtoday.eu/ Teachtoday-sivusto tarjoaa opettajille, rehtoreille ja muille koulun työntekijöille tietoa ja neuvoja uuden teknologian positiiviseen, vastuulliseen ja turvalliseen hyödyntämiseen.

Sivustolla olevien tapausesimerkkien avulla kouluttajat voivat herättää keskustelua osallistujien kohtaamista todellisista ongelmista kouluissa.
www.teachtoday.eu/en/Case-studies.aspx

	Christina Salmivallin videoluento onnistuneesta kiusaamisen vastaisesta kampanjasta Suomessa: www.youtube.com/watch?v=x6FkNkDp018 Cyberbullying – protecting kids and adults from online bullies (Samuel McQuade, Praeger, 2009) Cyberbullying and eSafety – what educators and other professionals need to know (Adrienne Katz, Jessica Kingsley Publishers, 2012) School Climate 2.0 – preventing cyberbullying and sexting one classroom at a time (Sameer Hinduja and Justin Patchin, Corwin, 2012) **Seksiviestittelyyn liittyviä materiaaleja** ”Handbook for schools: Sexual violence in digital media” www.saferInternet.at/chadvice/ ja englanniksi www.saferinternet.at/uploads/tx_simaterials/Sex_and_Violence_in_Digital_Media.pdf **Materiaali "So you got naked online?"** www.swgfl.org.uk/sextinghelp ja siihen liittyvä CEOP:in video "Exposed" http://www.youtube.com/watch?v=4ovR3FF_6us **Seksiviestittelyä käsittelevä näytelmä** www.childnet.com/kia/secondary/toolkit-advanced/picture-this.aspx
Arviointivaihtoehdot	• Osallistujat keskustelevat kokemuksistaan ennakkotehtävään liittyen ja kokemuksiensa yhteneväisyyksistä ja eroavaisuuksista. • Osallistujat tallentavat ja valikoivat materiaaleja koulujaan varten käyttämällä sosiaalista kirjanmerkkipalvelua. • Osallistujat twiittaavat materiaaleista, jota voivat käyttää kouluissaan, ja kirjoittavat niistä merkinnän oppimisblogiinsa.
Moduulin jälkeiset jatkotoimenpiteet	Ei ole.
Vaihtoehtoiset tavat toteuttaa moduuli	Jokaisessa tehtävässä on useita alakohtia. Jos osallistujat haluavat, kouluttajat voivat käyttää enemmän aikaa niihin sen sijaan, että siirryttäisiin eteenpäin seuraavaan tehtävään.
Toteuttamisvaihtoehdot kansallisella/paikallisella tasolla	Tämä moduuli voidaan toteuttaa kansallisella/paikallisella tasolla. Osallistujat voivat työskennellä eri kouluissa ja/tai opettaa eri oppiaineita. Kouluttajien tulee jakaa materiaaleja paikallisella kielellä aina kun mahdollista – www.saferinterent.org-sivuston ja Learning Resource Exchange -portaalin Insafe-osion käyttö auttaa tässä. http://lreforschools.eun.org/web/guest/insafe Moduuli sopii myös rehtoreille sekä opinto- tai oppilaanohjaajille.
Tehtävä 6.1:	**Mitä on virtuaalinen kiusaaminen?**
Kesto	50 min

Tavoitteet	• Keskustella virtuaalisesta kiusaamisesta, tarkastella virtuaalisia kiusaamistapauksia ja antaa osallistujien jakaa omien koulujensa kokemuksia • Selvittää, kuinka yleistä kiusaaminen/virtuaalinen kiusaaminen on. • Tarkastella koulun tietojärjestelmien käyttöehto ja /toimintasuunnitelmia/ käytäntöjä kiusaamisen estämiseksi.
Kuvaus	PowerPoint-esitys eS 6.1 Mitä on virtuaalinen kiusaaminen? Pptx muodostaa perustan tehtävälle 6.1. Se sisältää linkkejä videoihin ja alla luetelluille verkkosivustoille. **Tehtävä 1** Kouluttaja aloittaa istunnon esittämällä Common Sense Median videon: http://m.commonsensemedia.org/educators/cyberbullying-toolkit. Videossa esitellään maksuton virtuaalisen kiusaamisen ehkäisyn työkalupakki (Cyberbullying Toolkit) ja tarkastellaan opettajien roolia virtuaalisessa kiusaamisessa. Videossa korostetaan, että usein opettajat ovat ensimmäinen taho, joka voi auttaa uhriksi joutuneita oppilaita. 1. Kouluttaja varaa aikaa lyhyelle keskustelulle, jotta osallistujat voivat kertoa mielipiteensä lisävelvollisuuksista, joita opettajille saattaa tulla digitaaliseen turvallisuuteen ja erityisesti virtuaaliseen kiusaamineen liittyvissä asioissa. Kouluttajien on tärkeä huomata, että Euroopan unionin eri maissa on hyvin erilaisia tapoja toimia. Joidenkin opettajien mielestä virtuaalinen kiusaaminen ei kuulu heidän vastuulleen, ja siihen liittyviä asioita hoitavat koulun opinto- tai oppilaanohjaaja tai koulukuraattori. 2. Kouluttaja mainitsee, että osallistujat voivat rekisteröityä maksuttomien materiaalien käyttäjiksi ja perehtyä työkalupakin tuntisuunnitelmiin ja materiaaleihin tarkemmin seuraavassa tehtävässä. **Tehtävä 2** Virtuaalisen kiusaamisen määrittely. Kouluttaja pyytää ryhmää osallistumaan virtuaalisen kiusaamisen määrittelyyn ja esittää ryhmälle joitakin viimeisimpiä tutkimustuloksia aiheesta. Lähteinä voi käyttää seuraavia: EU Kids Online, Beatbullying Virtual Violence www.beatbullying.org/pdfs/Virtual%20Violence%20%20Protecting%20Children%20from%20Cyberbullying.pdf Lisää tietoa osoitteesta http://old.digizen.org/cyberbullying/fullguidance ja http://cyberbullying.us/ **Tehtävä 3** Kouluttaja esittelee tapaustutkimus virtuaalisesta kiusaamisesta: esim. Let's Fight it Together www.digizen.org/resources/cyberbullying/films/uk/lfit-film.aspx – tällä videolla on kiusaamistilanteessa eri rooleissa olevien haastatteluja. **TAI** Kouluttaja käyttää tosielämän esimerkkejä, esimerkiksi Ryan Halligan www.ryanpatrickhalligan.org tai Amanda Todd www.youtube.com/watch?v=KRxfTyNa24A. Kouluttaja antaa osallistujille mahdollisuuden keskustella videosta. **Keskustelua:** Miten nämä tapaukset olisi voitu estää – oliko mitään varoitusmerkkejä, mitä olisi voitu tehdä eri tavalla jne.? Ketkä ovat keskeisessä roolissa tämän tyyppisissä tapauksissa – ryhmä keskustelee jokaisen asianosaisen roolista. Kouluttaja näyttää videon http://www.youtube.com/watch?v=rpOvYWd4KW4, "We are all Daniel Chu", ja ryhmä

	keskustelee sivustakatsojan ja kiusatun puolustajan rooleista. **Tehtävä 4** Kouluttaja käyttää world cafe -menetelmää ja pyytää osallistujia keskustelemaan pienryhmissä siitä, mitkä asiat ovat etusijalla, kun kouluissa valistetaan virtuaalisesta kiusaamisesta. Kouluttaja jakaa paperia ja kyniä. Osallistujat hyödyntävät keskustelussa ennakkotehtävää ja oman koulunsa tietojärjestelmien käyttöehtoja. Kouluttaja varaa hetken aikaa ryhmien kommenteille ja erilaisten näkemysten jakamiselle.
Tehtävä 6.2:	**Koko koulun tapa puuttua virtuaaliseen kiusaamiseen**
Kesto	35 min
Tavoitteet	• Ymmärtää virtuaalisen kiusaamisen eri muotoja, erityisesti tahatonta virtuaalista kiusaamista. • Tutkia erilaisia aineistoja, jotka on tarkoitettu virtuaalisen kiusaamisen ehkäisyyn ja käsittelyyn. • Pohtia, miten virtuaalista kiusaamista ehkäisevät toimintasuunnitelmat vaativat koko koulun sitoutumista.
Kuvaus	**Tehtävä 1** Osallistujat tekevät tehtävän "Tunnebarometri", joka auttaa havainnollistamaan, miten eri ihmiset reagoivat verkossa kirjoitettuihin kommentteihin jne. Ennen tehtävää kouluttajan täytyy tulostaa osallistujille sopiva määrä kortteja seuraavasta linkistä: www.saferinternet.org/c/document_library/get_file?uuid=254ad474-4649-4661-95ff-871a4b326836&groupId=10137. (Linkki on saatavilla myös materiaalissa eS 6.2b, jos osallistujat haluavat käyttää sitä luokissaan.) **Tehtävä 2** Kouluttaja esittelee materiaalin eS 6.2b Virtuaaliseen kiusaamiseen ja seksuaalissävytteiseen viestittelyyn liittyviä aineistoja. Kouluttaja antaa osallistujille aikaa tutkia virtuaaliseen kiusaamiseen liittyviä aineistoja. Kannettavia tietokoneita käyttävät osallistujat 1. Osallistujat selaavat joitain alla olevia aineistoja ja tallentavat hyödylliset linkit sosiaaliselle kirjanmerkkitililleen. Kouluttaja nostaa esille sivuston www.cyberbullying.us ja sen vinkit teini-ikäisten virtuaalisen kiusaamisen ehkäisemiseen. 2. Osallistujat etsivät virtuaaliseen kiusaamiseen liittyviä aineistoja omalla kielellään oman maansa Safer Internet Awareness Centre www.saferinternet.org -sivuston ja Learning Resource Exchange -portaalin Insafe-osion avulla. http://lreforschools.eun.org/web/guest/insafe **Tehtävä 3** Kouluttaja esittelee tapaustutkimuksen Charliesta eS 6.2c Tapaustutkimus virtuaalisesta kiusaamisesta ja antaa osallistujien keskustella siitä. **Keskustelunaiheita:** Mitä olisi voitu tehdä toisin? Olisiko koulu voinut tehdä jotain enemmän? On tärkeää huomata, että koulu ei ollut aikaisemmin tarjonnut digitaaliseen turvallisuuteen ja virtuaaliseen kiusaamiseen liittyvää koulutusta. Oppilaiden kommenteista kävi ilmi, että he eivät olleet koskaan ajatelleet, miten eri lailla eri ihmiset voivat reagoida verkkoon kirjoitettuihin kommentteihin.

Kahvitauko	**10 min**
Tehtävä 6.3:	**Seksiviestittely - ongelmat ja haasteet**
Kesto	40 min
Tavoitteet	Tarkastella seksuaalissävytteiseen viestittelyyn liittyviä ongelmia, joita nuoret voivat kohdata verkossa.
Kuvaus	• Nopena alustuksena aiheeseen kouluttaja käyttää materiaalia eS 6.3 Seksuaalissävytteinen viestittely ja moraalinen kompassi pptx ja näyttää lyhyen videon seksuaalissävytteisestä viestittelystä, esim. Sheeplive.eu:n video "Coatless". • Sen jälkeen kouluttaja esittelee lyhyesti viimeisimpiä tutkimustuloksia aiheesta: EU Kids Online, NSPCC, Plymouthin yliopisto, Itävallan Safer Internet Centre. Lisäksi osallistujia pyydetään jakamaan omia kokemuksiaan, jotta voidaan tunnistaa keskeisimmät ongelmat ja kysymykset. • Kouluttaja näyttää ensimmäisen osan kouluille tarkoitetuista opetussuunnitelma-aineistoista - Mikä tahansa video osiosta Seksiviestittelyä käsittelevä aineisto, jotka on lueteltu aiemmassa materiaalissa eS 6.2b Virtuaaliseen kiusaamiseen ja seksuaalissävytteiseen viestittelyyn liittyviä aineistoja. Videoista voi näyttää esimerkiksi videon *Tagged, Exposed, First to a million.* Nämä ovat oppituntiaineistoa, johon sisältyy tuntisuunnitelmat ja jatkotehtävät. **Tehtävä - Moraalikompassi** Keskustelu aiheesta käynnistetään tekemällä moraalikompassitehtävä. Kouluttajan täytyy tulostaa piilotetut diat pptx-tiedoston lopusta ja kiinnittää kahdeksan kompassisuuntaa eri puolille huonetta. Ne edustavat eri mielipiteitä, joita osallistujilla on aiheeseen liittyvistä väittämistä. (Tehtävää voidaan teettää myös oppilailla kouluissa.) Kouluttaja lukee ääneen yhden seuraavista väittämistä: • Alastonkuvan lähettäminen poikaystävälle tai tyttöystävälle on hyväksyttävää, kun kaksi ihmistä seurustelee keskenään. • Seksuaalissävytteisten kuvien lähettämisestä matkapuhelimella tulisi keskustella kouluissa • Seksiviestittelyn pahin puoli on kuvan pysyvyys ja se, ettei sitä koskaan saa poistettua lopullisesti.) Osallistujat menevät huoneessa sen kompassisuunnan kohdalle, joka edustaa heidän näkemystään. Sen jälkeen kouluttaja pyytää osallistujia selittämään, miksi he menivät seisomaan tiettyyn kohtaan ja miksi he ovat sitä mieltä. Ryhmä pohtii yhdessä voidaanko digikansalaisuutta, netikettiä ja empatiaa opettaa.

Tehtävä 6.4:	**Seksiviestittely - ehkäisevät toimet ja tukeminen**
Kesto	30 min
Tavoitteet	• Ehdottaa erilaisia tapoja puuttua seksuaalissävytteiseen viestittelyyn sekä seksuaalisuuteen ja Internetiin liittyviin ongelmiin kouluissa. • Tarjota mahdollisuus tutustua erilaisiin aineistoihin, joita on saatavilla koulujen työn tueksi.
Kuvaus	Sen jälkeen, kun moraalikompassitehtävän yhteydessä on keskusteltu digikansalaisuuden, netiketin ja empatian opettamisesta, kouluttaja pyytää osallistujia kertomaan ajatuksiaan ja kokemuksiaan siitä, miten ottaa esiin seksuaalissävytteiseen viestittelyyn ja Internetiin liittyvät seksuaaliset kysymykset ja ongelmat luokassa. • Onko se ongelma? • Mikä ympäristö sopii aiheesta keskustelulle? • Keiden tulisi olla kohderyhmä? • Mitä aineistoja ja materiaaleja opettajat voivat käyttää oppilaiden tukemiseksi? Kouluttaja mainitsee käsikirjan ”Handbook for Educators: Sexual Violence in Digital Media”, joka on listattu aiemmassa materiaalissa, eS 6.2b Virtuaaliseen kiusaamiseen ja seksuaalissävytteiseen viestittelyyn liittyviä aineistoja. Se sisältää tuntisuunnitelmia ja tehtäviä; kouluttaja mainitsee myös britannialaiset aineistot, esim. CEOP:in video "Exposed", joista saa apua seksiviestittelytapausten käsittelyyn: eS 6.4b So you got naked online? Eri maiden välillä on eroja erityisesti seksuaalissävytteiseen viestittelyyn liittyvissä oikeudellisissa kysymyksissä ja kuinka lainsäädäntö suhtautuu siihen. Tämä näkökulma on tärkeää huomioida keskustelussa.
Tehtävä 6.5	**Oppimisen pohdintaa**
Kesto	10 min
Tavoitteet	Tehdä yhteenveto osallistujien päivän aikana oppimista asioista ja siitä, miten he aikovat ryhtyä soveltamaan opittua käytäntöön kouluissa.
Kuvaus	Osallistujien itsearviointia oppimispäiväkirjaan. • Mitä olen oppinut tänään? • Mitä tietoa jaan kollegoilleni koulussa? Osallistujat voivat kirjata ajatuksiaan ja huomioitaan moduulin 6 tukimateriaalista. Osaavatko he nimetä ja jakaa omalla äidinkielellään olevia aineistoja?

Moduuli 6: KURSSIN TUKIMATERIAALIT

Kurssi/Moduuli/Tehtävä	Kurssin tukimateriaalit
eS 6.1	Mitä on virtuaalinen kiusaaminen? pptx
eS 6.2b	Virtuaaliseen kiusaamiseen ja seksuaalissävytteiseen viestittelyyn liittyviä aineistoja (pdf)
eS 6.3	Seksuaalissävytteinen viestittely ja moraalinen kompassi pptx
Tukimateriaalia	Nämä aineistot voidaan laittaa saataville kurssin verkko-oppimisympäristöön tai oppimisalustalle.
eS 6.4b	Materiaali "So you got naked online?" (pdf)
eS 6.2c	Tapaustutkimus virtuaalisesta kiusaamisesta (pdf)

Kouluttajan käsikirja ja tukimateriaalit

Kurssi:

Digitaalinen turvallisuus: TURVALLISEMPI KOULU JA LUOKKAYMPÄRISTÖ

Moduuli 7: Käytännön lähestymistapoja digitaaliseen turvallisuuteen oppitunneilla

(eS 7.0)

eS 7.0: Käytännön lähestymistapoja digitaaliseen turvallisuuteen oppitunneilla

CPDLab-kurssi	**Digitaalinen turvallisuus: Digitaalisen turvallisuuden parantaminen kouluissa**
Moduulin numero	**eS 7.0**
Moduulin nimi	**Käytännön lähestymistapoja digitaaliseen turvallisuuteen oppitunneilla**
Vaatimukset moduulin suorittamiseen	Osallistujilla tulee olla • perustaidot tieto- ja viestintätekniikan käytössä ja kiinnostus digitaalisen teknologian ja Internetin käyttöön opetuksessa ja oppimisessa. • jonkinlainen tuntemus sosiaalisen median palveluista, niiden toiminnasta ja käytöstä. Ihanteellista olisi, jos osallistujat ovat suorittaneet moduulit 1 ja 2. • kiinnostus siitä, miten interaktiiviset ja yhteistoiminnalliset pedagogiset työkalut, kuten bloggaus, wikit, eTwinning ja virtuaaliset oppimisympäristöt, voivat tehostaa opetusta ja oppimista, kun opettaja näyttää mallia ja moderoi näiden työkalujen käyttöä. Osallistujat tarvitsevat tilapäisen sähköpostiosoitteen, jonka avulla he voivat rekisteröityä erilaisiin sosiaalisen median palveluihin ja kokeilla niitä. Tähän tarkoitukseen ei pitäisi käyttää henkilökohtaista sähköpostiosoitetta tai koulun tai työpaikan sähköpostiosoitetta. Heillä tulisi olla pääsy kurssin verkkoalueille, oppimispäiväkirjaan ja kurssin tukimateriaaleihin, moduulin 1 aikana perustettu käyttäjätili sosiaalisessa kirjanmerkkipalvelussa sekä moduulin 3 aikana perustettu Twitter-tili.
Kesto	3 tuntia
Kurssipaikka ja moduulin rakenne	Tämä moduuli järjestetään lähiopetuksena. Osallistujat työskentelevät pienryhmissä ja käyttävät työn tulosten esittelemiseen tietokoneita ja muita laitteita, kuten kosketustaulua. Moduuli sisältää käytännön tehtäviä, keskustelua ja ryhmätöitä.
Tarvittavat tilat ja tilajärjestelyt	• Tehtäviä varten tarvitaan 5 - 6 arkkia fläppitaulun paperia ja sinitarraa. • Kouluttaja tarvitsee käyttöönsä kosketustaulun, tietokoneen ja langattoman verkon. • Jokainen osallistuja tarvitsee käyttöönsä tietokoneen, jossa on Internet-yhteys. • Tiloissa tulisi olla tarpeeksi virtapistokkeita kannettaville tietokoneille. Lisäksi osallistujat tarvitsevat tiloja, joihin hajaantua työsken-

	telemään 3–5 hengen pienryhmissä.
Moduulin yleiskuvaus	Osallistujat arvioivat oppimisessa käytettävää tieto- ja viestintätekniikkaa. He perehtyvät työkaluihin, jolla oppilaat voivat esittää tietoa esityksen tarkoitukseen, yleisön tarpeisiin ja sisältöön sopivassa muodossa. He tarkastelevat työkalujen turvallisuusominaisuuksia ja oppivat arvioimaan niihin liittyviä riskejä. Osallistujat suunnittelevat alustavia digitaalisen turvallisuuden opetustuokioita (idea, rakenne) oppilaille ja etsivät verkosta sopivia oppimisvälineitä ja -aineistoja opetustuokiota varten. Osallistujat oppivat mukauttamaan tuntisuunnitelmia oppilailleen sopiviksi ja etsimään ja valikoimaan digitaalisen turvallisuuden oppimateriaaleja ja opetussuunnitelmia. Osallistujat etsivät myös aineistoja omalla kielellään Insafe- ja Safer Internet Awareness Centre -sivustoja sekä Learning Research Exchange -portaalia hyödyntäen http://lreforschools.eun.org/web/guest/insafe
Moduulin tavoitteet	• Määrittää tarve koko koulun asteittain etenevälle digitaalisen turvallisuuden opetussuunnitelmalle • Tarkastella mitä hyötyä saadaan, kun oppilaille annetaan tehtäväksi hyödyntää bloggaamista, wiki-sivustoja, keskustelufoorumeita ja muita digitaalista mediaa opittavien asioiden pohdinnassa • Jakaa pedagogista tietoutta ja erilaisia malleja opetuksen ja oppimisen toteuttamiseen • Luoda opetussuunnitelmaan tuntisuunnitelmia digitaalisen turvallisuuden opettamiseksi koulussa.
Taitojen ja osaamisen karttuminen moduulissa	Osallistujat oppivat • sisällyttämään digitaalisen turvallisuuden käytännöt osaksi tieto- ja viestintätekniikan opetusta • käyttämään digitaalista teknologiaa opetukseen luokkaympäristössä kehittämään oppilaiden digitaalista lukutaitoa ja digikansalaistaitoja • muokkaamaan Internetistä saatavaa materiaalia opetuksen suunnittelua varten • etsimään ja valikoimaan materiaaleja ja aineistoja, joita voi käyttää digitaalisen turvallisuuden opettamisessa oppilaille.
Tarvittavat materiaalit ja välineet	• Monisteet eS 7.2 : eS 7.4 • Fläppitaulupaperia ja sinitarraa. • Kouluttajalle tietokone, jossa on Internet-yhteys, ja dataprojektori. • Osallistujille kannettavat tietokoneet ja pääsy langattomaan verkkoon. • Kosketustaulu tulosten esittämiseen. • Pääsy kurssin tukimateriaaleihin ja oppimispäiväkirjaan.

Vaatimukset kouluttajalle	Ennen moduulin alkua kouluttaja voi perustaa ilmaisen tilin Collaborize Classroom -palveluun (www.collaborizeclassroom.com) ja tutustua sen keskustelunavauksiin digikansalaisuudesta, esim. *kuinka chattailla, keskustella ja kommentoida.* Kouluttajalla tulee olla syvällinen ja monipuolinen tietämys digitaalisesta lukutaidosta, digitaaliseen turvallisuuteen liittyvistä kysymyksistä ja digitaalisen turvallisuuden opetussuunnitelmista. Kouluttajan tulee tuntea Eu-politiikka, jonka tavoitteena on tehdä Internetistä turvallisempi lasten ja nuorten näkökulmasta, Insafen materiaalit ja palvelut sekä paikallisen Safer Internet Centren materiaalit ja kansainvälinen digitaalisen turvallisuuden opetussuunnitelma. Kouluttajan tulee tutustua kurssin verkkoalueeseen ja kaikkiin kurssin tukimateriaaleihin, jotka on lueteltu jokaisen moduulin lopussa. Jokainen materiaali on luetteloitu kurssin, moduulin ja tehtävän mukaan, esim. eS 1.1 "Ihmisbingo digikansalaisille" Kouluttajan tulee käyttää sosiaalista kirjanmerkkipalvelua (esim. www.delicious.com tai Diigo www.diigo.com) digitaaliseen turvallisuuteen liittyvien linkkien ja materiaalien tallentamiseksi. Kouluttajan tulee myös kannustaa osallistujia luomaan oma käyttäjätilinsa, jonka avulla he voivat hallita kurssilla käsiteltyjä verkkoaineistoja. Kouluttajan tulee tietää, kuinka Twitteriä, sosiaalisia kirjanmerkkipalveluita ja blogeja käytetään, ja perustaa oppimisblogi ennen kurssia.
Lähdeaineistot ja materiaalit kouluttajalle	**Collaborize Classroom, maksuton keskustelufoorumi opetuskeskusteluille**: www.collaborizeclassroom.com **Kathy Schrockin opas Kathy Schrock Guide to Everything:** www.schrockguide.net **Hakukone digitaalisten työkalujen etsimiseen**. http://itools.com/ - **Learning Research Exchange -portaali** http://lreforschools.eun.org/web/guest/insafe **Esimerkkejä opetussuunnitelmasta** Creative Commons Media www.commonsensemedia.org/educators/lesson/my-creative-work-k-2 **Digitaalinen lukutaito** www.swgfl.org.uk/digitalliteracy **Cable and Wireless opetussuunnitemat** www.ciconline.org/DigitalCitizenship Media Smarts: http://mediasmarts.ca/digital-media-literacy-fundamentals **Google/YouTube-opetussuunnitelma** www.google.com/edu/teachers/youtube/curric/ **Ilmainen digitaalisen turvallisuuden opetussuunnitelma** www.commonsensemedia.org/educators/curriculum

	Ilmainen opetussuunnitelma Australian valtionhallinnon sivustolla www.cybersmart.gov.au/Schools.aspx **Linkkejä Microsoftin opetussuunnitelmaan** http://edudemic.com/2012/10/teachers-guide-digital-citizenship/ **Insafe** www.saferInternet.org Osittain Euroopan unionin rahoittama Insafe on eurooppalainen Safer Internet Centre -verkosto, joka edistää turvallista ja vastuullista Internetin ja mobiililaitteiden käyttöä nuorten keskuudessa. Se tarjoaa laajan valikoiman materiaaleja ja tietolähteitä useilla eri kielillä. Jokaisella jäsenmaalla on oma **Safer Internet Awareness Centre.** On mahdollista hyödyntää myös muiden maiden (esimerkiksi englannin- tai ruotsinkielisiä) Safer Internet Awareness Centre-aineistoja. **Safer Internet Day** (SID) www.saferInternetday.org Helmikuun toisena tiistaina vietetään kouluissa vuosittain kansainvälistä Internet-turvallisuuden teemapäivää (Safer Internet Day). EU:n hanke tarjoaa materiaaleja, oppituntisuunnitelmia ja teemapaketteja opettajille ja kouluille. **Euroopan komissio** "Eurooppalainen strategia Internetin parantamiseksi lasten näkökulmasta", saatavana useilla eri kielillä: http://ec.europa.eu/information_society/activities/sip/policy/index_en.htm **Teach today** www.teachtoday.eu/ Teachtoday-sivusto tarjoaa opettajille, rehtoreille ja muille koulun työntekijöille tietoa ja neuvoja uuden tekniikan myönteiseen, vastuulliseen ja turvalliseen hyödyntämiseen. Sivustolla olevien tapausesimerkkien avulla kouluttajat voivat herättää keskustelua osallistujien kouluissaan kohtaamista todellisista ongelmista. www.teachtoday.eu/en/Case-studies.aspx **Byron Review –raportti** www.dcsf.gov.uk/byronreview "Safer Children in a Digital World" (Digitaalinen maailma turvallisemmaksi lapsille)
Arviointivaihtoehdot	• Osallistujat kirjoittavat ainakin yhden twiitin ryhmän Twitter-kanavalle. • Osallistujat jakavat julkisesti sosiaaliset kirjanmerkkitilinsä ja seuraavat kouluttajan ja ainakin yhden muun osallistujan kirjanmerkkejä.

Moduulin jälkeiset jatkotoimenpiteet	Digitaalisen turvallisuuden oppituntien valmistelu omille oppilaille. Webinaari, jossa osallistujat kertovat, kuinka he jakavat digitaalisen turvallisuuden tuntisuunnitelmiaan ja tietouttaan kollegojensa kanssa koululla.
Vaihtoehtoiset tavat toteuttaa moduuli	Ei vaihtoehtoisia toteuttamistapoja.
Toteuttamisvaihtoehdot kansallisella/paikallisella tasolla	Tämä moduuli voidaan toteuttaa kansallisella/paikallisella tasolla.
Tehtävä 7.1:	**Digitaalisten työkalujen opetus- ja oppimiskäyttö**
Kesto	1 h 10 min
Tavoitteet	• Tutkia oppimiseen käytetyn tieto- ja viestintätekniikan turvallisuusominaisuuksia. • Mahdollistaa interaktiivisten oppimistapojen turvallinen käyttö luokassa. • Kehittää digitaalisen turvallisuuden opetusta, joka auttaa oppilaita tekemään oikeita valintoja digitaalista teknologiaa käyttäessään. • Ymmärtää, kuinka oppilaat voi osallistaa aktiivisesti oppimisprosessiin ja samalla käyttää tieto- ja viestintätekniikkaa turvallisesti oppimisessa. • Jakaa hyviä digitaaliseen turvallisuuteen liittyviä pedagogisia strategioita ja käytäntöjä.
Kuvaus	Avaa materiaali eS 7.1 Digitaalisen luokkahuoneen työkalupakki pptx • **@Dia 4 Ryhmätyö** Osallistujat muodostavat kolme pienryhmää. Jokainen ryhmä valitsee yhden työkalun. Jos mahdollista, työkalun tulisi olla sellainen, mitä he eivät ole vielä käyttäneet opetuksessa. Kouluttaja varmistaa, että jokainen ryhmä valitsee eri työkalun. Kurssilla oppimaansa hyödyntäen ryhmät luovat Etherpad-sivun: http://etherpad.opensourcebridge.org tai Openetherpad-sivun http://openetherpad.org Kouluttaja voi näyttää dian 5 ja esitellä, mitä osallistujat voisivat tehdä tehtävässä 1. Laadi oppilaillesi lyhyt ohjeistus otsikolla: *Luokan blogin/wikin/keskustelufoorumin turvallinen käyttö.* **Tiedoksi kouluttajalle:** Pyydä keskustelufoorumin valinnutta ryhmää rekisteröitymään ja tutustumaan Collabarize Classroom -sivustoon, www.collaborizeclassroom.com **Palaute:** Ryhmät esittelevät lyhyesti etherpad-asiakirjansa ja lisäävät etherpad-linkit kurssin verkkoalueelle.

	• **@Dia 6** Jokainen ryhmä tai pari valitsee ilmaisen työkalun, etsii siitä tietoa Googlesta ja testaa työkalua keskustellen seuraavista asioista: 1) työkalun hyödyllisyys opetus- ja oppimiskäytössä 2) työkalun turvallisuusominaisuudet 3) työkalun käyttöön liittyvät riskit opettajan ja oppilaiden näkökulmasta. Jokainen ryhmä laatii etherpadin avulla ohjeet työkalun käyttöön otsikolla *Ohjeita opettajille (valitun työkalun) käyttöön*. **Palaute:** Ryhmät esittelevät lyhyesti etherpad-asiakirjansa ja lisäävät etherpad-linkit kurssin verkkoalueelle. Vaihtoehtoisesti ryhmä voi halutessaan valmistella Teachmeet-tyylisen tapaamisen kollegoilleen omassa koulussaan ja esitellä työkalun heille. Kouluttaja voi päättää osion antamalla osallistujille seuraavan linkin: http://itools.com/ - Hakukone digitaalisten työkalujen etsimiseen.
Tehtävä 7.2:	**Opetussuunnitelmaan pohjautuvan tuntisuunnitelman laatiminen omaan oppiaineeseen.**
Kesto	35 min
Tavoitteet	• Soveltaa digitaalisesta turvallisuudesta saatuja tietoja ja taitoja käytäntöön omassa opetuksessa. • Saada kokemusta digitaalisen turvallisuuden käytäntöjen, toimintatapojen tai ohjeiden sisällyttämisestä opetussuunnitelman mukaiseen oppituntiin. • Jakaa tuntisuunnitelmat. • Arvioida kurssin sisältöä tuntisuunnitelmien perusteella ja arvioida, ovatko osallistujien tuntisuunnitelmat sopivia digitaalisen turvallisuuden opetuksen toteuttamiseen heidän oman oppiaineensa yhteydessä. • Määrittää tarve koko koulun asteittain etenevälle digitaalisen turvallisuuden opetussuunnitelmalle.
Kuvaus	**Tehtävä** Jokainen osallistuja laatii tuntisuunnitelman *omaan oppiaineeseensa* käyttämällä tuntisuunnitelmapohjaa eS 7.2 Tuntisuunnitelmapohja. Tuntisuunnitelmasta tulee ilmetä osallistujien digitaaliseen turvallisuuteen liittyvät tiedot ja taidot ja sen tulee käsitellä oppilaiden kannalta merkityksellisiä digitaalisen turvallisuuden kysymyksiä.

	Osallistujat voivat • käyttää tuntisuunnitelmaa, jonka he ovat laatineet aiemmin tai jota he ovat käyttäneet aiemmin opetuksessaan • muokata jotain tuntisuunnitelmaa, joka on esitelty kurssin aikana • luoda tuntisuunnitelman jostain kurssilla käsitellystä digitaaliseen turvallisuuteen liittyvästä aiheesta, jonka he haluaisivat ottaa mukaan oppiaineensa opetussuunnitelmaan. Osallistujat voivat käyttää kaikkia kurssilla esiteltyjä aineistoja, kuten Insafe-verkoston käsikirjoja *The Web We Want* ja *Using the Mobile Phone in School*, paikallisen Safer Internet Awareness Centren verkkosivulla olevia aineistoja, Learning Resource Exchange -portaalia, omaa sosiaalista kirjanmerkkitiliään, kurssin tukimateriaalia sekä tietysti Internetiä ja Twitteriä. **30 minuutin kuluttua** – Kouluttaja ilmoittaa, että kahvitauon jälkeen jokainen osallistuja kertoo ryhmälle lyhyesti 1. opettamansa aineen ja oppilaidensa iän 2. oppituntinsa otsikon ja aiheen 3. mihin digitaaliseen turvallisuuteen liittyvään ongelmaan tai kysymykseen tuntisuunnitelma liittyy 4. pääasialliset aineistot, joita osallistuja hyödynsi oppitunnin kehittelyssä.
Kahvitauko	10 min
Tehtävä 7.3	**Käsitelläänkö oppitunneilla keskeisiä asioita?**
Kesto	20 min
Tavoitteet	• Esittää ryhmälle digitaalisen turvallisuuden huomioivan tuntisuunnitelman osallistujan itse opettamasta aineesta. • Perehtyä digitaalisen turvallisuuden aiheisiin, jotka kiinnostavat osallistujia eniten. • Pohtia digitaalisen turvallisuuden kysymyksiä, joita ei ole käsitelty osallistujien tuntisuunnitelmissa. • Keskustella siitä, kuinka nämä kysymykset voidaan huomioida digitaalisen turvallisuuden opetuksessa. • Tarkastella, kuinka digitaalinen turvallisuus voidaan ottaa osaksi koko koulun toimintaa ja keskustella siitä, kenen tulisi opettaa digitaalista turvallisuutta. • Arvioida kurssin sisältöä.
Kuvaus	Tämä tehtävä on jatkoa tehtävälle 7.3. **Tehtävä 1** Kouluttaja luo Padlet-tilan, ja jokainen osallistuja esittelee tuntisuunnitelmansa lyhyesti vastaamalla tehtävässä 7.3 esitettyihin neljään kysymykseen.

Kouluttaja laittaa jokaisen osallistujan kohdalle PadletNote-lapun, jossa mainitaan *ainoastaan*
a) opetettava aine ja
b) käsitelty digitaalisen turvallisuuden ongelma tai kysymys.

Tehtävä 2
Kun kaikki ovat vastanneet, kouluttaja pyytää osallistujia luokittelemaan Padletwall-seinälle luetellut digitaaliseen turvallisuuteen liittyvät aiheet ja ongelmat käyttämällä seuraavaa määritelmää digitaalisesta turvallisuudesta: Henkilökohtainen turvallisuus, Digitaalinen lukutaito ja Digikansalaisuus. Kouluttaja auttaa luokittelussa laatimalla kolme otsikkoa (Henkilökohtainen turvallisuus, Digitaalinen lukutaito ja Digikansalaisuus) ja kysyy, minkä otsikon alle kukin PadletNote-muistilappu siirretään.

Kouluttaja huomioi, mitkä osa-alueet, ongelmat tai kysymykset ovat jääneet käsittelemättä tuntisuunnitelmissa. (Tyypillisesti opettajat ylikorostavat digitaalista lukutaitoa ja henkilökohtaista turvallisuutta, ja digikansalaisuus mainitaan harvemmin.)

Ryhmä keskustelee, mitkä aiheet olivat suosituimpia ja mitkä digitaaliseen turvallisuuteen liittyvät kysymykset jäivät kokonaan tai lähes kokonaan huomioimatta.
Kouluttaja yrittää löytää osallistujien kanssa syyn siihen, miksi joitakin digitaalisen turvallisuuden kysymyksiä tai ongelmia ei käsitelty.

- Mitä ne ovat? Mitä ongelmia ja kysymyksiä on käsitelty kurssin moduuleissa tähän mennessä?
- Voivatko osallistujat luokitella ne?
- Kuinka voimme varmistaa, että näitä ongelmia ja kysymyksiä käsitellään kouluissa?
- Kenen tulisi olla vastuussa niiden opettamisesta?
- Mitä näistä ongelmista ja kysymyksistä kaikkien opettajien tulisi käsitellä tunneillaan?
- Mihin oppiaineisiin voidaan sisällyttää keskeiset kysymykset?
- Onko osallistujien kotimaan koulutusjärjestelmässä sellaisia oppiaineita kuin sosiaaliset taidot/yhteiskuntaoppi/terveystieto?
- Voimmeko jättää digitaalisen turvallisuuden opetuksen vain tieto- ja viestintätekniikan opettajan vastuulle? Ohjaa osallistujia keskustelemaan koko koulun kattavan digitaalisen turvallisuuden opetussuunnitelman tarpeesta.

Huom.: Jos on aikaa, niin ryhmä voi halutessaan jakaa tehtävän **7.3** tuntisuunnitelmia sen mukaan, mitkä suunnitelmat ovat heidän mielestään erityisen hyödyllisiä ja mitä suunnitelmia he haluaisivat käyttää omien oppilaidensa kanssa. Kurssin oppimisalustalle voidaan luoda kansio hyödyllisimmiksi koettujen aineistojen jakamiseen.

Tehtävä 7.4	**Digitaalisen turvallisuuden opetussuunnitelman laatiminen koko koululle**
Kesto	40 min
Tavoitteet	• Tarkastella olemassa olevia koko koulun digitaalisen turvallisuuden opetussuunnitelmia. • Muokata ja sovittaa valmis opetussuunnitelma osallistujan oman koulun käyttöön sopivaksi. • Laatia asteittain etenevä digitaalisen turvallisuuden opetussuunnitelma jokaisen osallistujan omaan kouluun.
Kuvaus	**Tehtävä** Kouluttaja pyytää osallistujia muodostamaan pienryhmiä sen perusteella, mitä luokka-astetta he opettavat (esim. 1–6 luokka). Näissä ryhmissä osallistujat laativat digitaalisen turvallisuuden opetussuunnitelman koko koululle. **Tiedoksi kouluttajille** Yritä saada osallistujia jokaiselta luokka-asteelta, niin että 2 - 3 osallistujaa käsittelee kutakin luokka-astetta ja lopputuloksena on asteittain etenevä koko koulun opetussuunnitelma. Esimerkki ensimmäistä luokkaa koskevasta digitaalisen turvallisuuden opetussuunnitelmasta on annettu materiaalissa eS 7.4. Jaa seuraava materiaali: eS 7.4 Ehdotus oppiainerajat ylittäväksi koko koulun digitaalisen turvallisuuden opetussuunnitelmaksi (doc) Pidä Padlet-sovelluksessa luokitellut aiheet näkyvissä ja kehota osallistujia arvioimaan olemassa olevia koko koulun opetussuunnitelmia, joita on käsitelty kurssilla ja tallennettu sosiaaliselle kirjanmerkkitilille. **Kouluttaja** kehottaa osallistujia käyttämään EU:n laatimia sekä kansallisista ja kansainvälisistä lähteistä saatavia esimerkkiopetussuunnitelmia. Kouluttaja kiinnittää seinälle 5 - 6 suurta paperia, yhden jokaista luokka-astetta kohden. Kun osallistujat ovat saaneet valmiiksi ehdotuksensa luokka-asteen opetussuunnitelmaksi, he kirjoittavat sen paperille, ja tutustuvat toistensa opetussuunnitelmiin.
Lounas	1 tunti

Moduuli 7: KURSSIN TUKIMATERIAALIT

Kurssi/Moduuli/Tehtävä	Kurssin tukimateriaalit
eS 7.1	Digitaalisen luokkahuoneen työkalupakki pptx
eS 7.2	Tuntisuunnitelmapohja doc [Moniste]

Kouluttajan käsikirja ja tukimateriaalit

Kurssi:

Digitaalinen turvallisuus: TURVALLISEMPI KOULU JA LUOKKAYMPÄRISTÖ

Moduuli 8: Digitaalinen turvallisuus koulun opetussuunnitelmassa ja sen ulkopuolella

(eS 8.0)

eS 8.0: Digitaalinen turvallisuus koulun opetussuunnitelmassa ja sen ulkopuolella

CPDLab-kurssi	**Digitaalinen turvallisuus: Digitaalisen turvallisuuden parantaminen kouluissa**
Moduulin numero	**eS 8.0**
Moduulin nimi	**Digitaalinen turvallisuus koulun opetussuunnitelmassa ja sen ulkopuolella**
Vaatimukset moduulin suorittamiseen	• Moduulissa 8 käsitellään loppuun moduulissa 7 esitellyt digitaalisen turvallisuuden suunnitelmat ja lähestymistavat. • Osallistujat ovat aiemmin osallistuneet digitaalisen turvallisuuden kurssille ja suorittaneet erityisesti moduulin 7. • Osallistujilla tulee olla perustaidot tieto- ja viestintätekniikan käytössä ja kiinnostus digitaalisen teknologian ja Internetin käyttöön opetuksessa ja oppimisessa. • Heidän tulisi olla kiinnostuneita siitä, miten opetusta ja oppimista voidaan tehostaa interaktiivisen sosiaalisen median pedagogisten työkalujen, kuten bloggauksen, eTwinningin ja virtuaalisten oppimisympäristöjen avulla opettajan näyttäessä mallia ja moderoidessa työkalujen käyttöä. • Osallistujien tulisi tuntea Insafe-verkoston toimintaa ja kansallisia ja kansainvälisiä digitaalisen turvallisuuden opetussuunnitelmia ja ohjelmia.
Kesto	3 tuntia
Kurssipaikka ja moduulin rakenne	• Tämä moduuli järjestetään lähiopetuksena. • Osallistujia kehotetaan ottamaan mukaan oma kannettava tietokoneensa, sillä moduulin aikana kokeillaan opetettavia asioita käytännössä. • Sen lisäksi moduuliin kuuluu tehtäviä, keskustelua, ryhmätöitä ja pohdintaa.
Tarvittavat tilat ja tilajärjestelyt	• Kouluttaja tarvitsee käyttöönsä kosketustaulun, tietokoneen ja Internet-yhteyden. • Osallistujat tarvitsevat kannettavat tietokoneet ja langattoman verkkoyhteyden, salasanat kurssin verkkoalueelle ja oppimisblogiin (kouluttaja luo blogin Wordpressiin tai vastaavaan palveluun ennen kurssin alkua). • Lisäksi tarvitaan koulutustila sekä työskentelytiloja pienryhmille.
Moduulin yleiskuvaus	Osallistujat perehtyvät moduulissa 7 laadittuihin opetussuunnitelmaehdotuksiin, äänestävät suosikkiaan ja keskustelevat siitä, kuinka opetussuunnitelma voitaisiin porrastaa kaikille luokka-asteille ja tehdä siitä näin asteittain etenevä. Osallistujat keskustelevat ja suunnittelevat myös, kuinka kurssilla saadut digitaaliseen turvallisuuteen liittyvät tiedot ja taidot voitaisiin siirtää kollegoille koulussa sekä oppilaille ja heidän vanhemmilleen.

Moduulin tavoitteet	• tarkastella Internet-turvallisuuden teemapäivän tuomia hyötyjä koulussa • ymmärtää, kuinka osallistaa vanhemmat koulun digitaalisen turvallisuuden ohjelmaan • laatia omalle koululle sopiva, asteittain etenevä digitaalisen turvallisuuden opetussuunnitelma.
Taitojen ja osaamisen karttuminen tässä moduulissa	Osallistujat oppivat • soveltamaan kurssilla saatuja taitoja ja osaamista digitaalisen turvallisuuden opetuksessa • laatimaan omalle koululleen asteittain etenevän opetussuunnitelman • jakamaan valmiita materiaaleja ja suunnitelmia kollegojensa kanssa • osallistamaan oppilaat ja vanhemmat koulun digitaalisen turvallisuuden ohjelmaan.
Tarvittavat materiaalit ja välineet	• Sinitarraa, tusseja ja Post-it-lappuja • Monisteet eS 8.5a ja eS 8.5b • Kouluttajalle tietokone, jossa on Internet-yhteys, ja dataprojektori. • Osallistujille kannettavat tietokoneet ja pääsy langattomaan verkkoon. • Kosketustaulu tulosten esittämiseen. • Pääsy kurssin tukimateriaaleihin ja oppimispäiväkirjaan.
Vaatimukset kouluttajalle	Kouluttajalla tulee olla syvällinen ja monipuolinen tietämys digitaalisesta lukutaidosta, digitaaliseen turvallisuuteen liittyvistä kysymyksistä ja digitaalisen turvallisuuden opetussuunnitelmista. Kouluttajan tulee tuntea Eu-politiikka, jonka tavoitteena on tehdä Internetistä turvallisempi lasten ja nuorten näkökulmasta, Insafen materiaalit ja palvelut sekä paikallisen Safer Internet Centren materiaalit ja kansainvälinen digitaalisen turvallisuuden opetussuunnitelma. Kouluttajan tulee tutustua kurssin verkkoalueeseen ja kaikkiin kurssin tukimateriaaleihin, jotka on lueteltu jokaisen moduulin lopussa. Jokainen materiaali on lueteloitu kurssin, moduulin ja tehtävän mukaan, esim. eS 1.1 "Ihmisbingo digikansalaisille" Kouluttajan tulee käyttää sosiaalista kirjanmerkkipalvelua (esim. www.delicious.com tai Diigo www.diigo.com), jonne tallennetaan digitaaliseen turvallisuuteen liittyviä linkkejä ja materiaaleja. Kouluttajan tulee myös kannustaa osallistujia luomaan oma käyttäjätili kurssilla jaettujen verkkomateriaalien hallinnoimiseksi. Kouluttajan tulee perustaa oppimisblogi ja antaa sen käyttäjätunnukset ja salasana osallistujille. Sen lisäksi kouluttajan täytyy osata käyttää ryhmätyösovelluksia, blogeja, padletia ja vastaavia sovelluksia. Kouluttajan tulee hallita Twitterin käyttö.
Lähdeaineistoja ja materiaaleja kouluttajille	**Kathy Schrockin opas Kathy Schrock's Guide to Everything:** www.schrockguide.net Katso erityisesti osiot Critical thinking ja Information literacy

	Read, Write, Think www.readwritethink.org/professional-development/strategy-guides/reading-online-30096.html **The Talent Show** www.youtube.com/watch?v=bdQBurXQOeQ Juttele ja kommentoi verkossa aivan kuten oikeassa elämässä. **Safer Internet Day** (SID) www.saferInternetday.org Helmikuun toisena tiistaina vietetään kouluissa vuosittain kansainvälistä Internet-turvallisuuden teemapäivää (Safer Internet Day). EU:n hanke tarjoaa materiaaleja, oppituntisuunnitelmia ja teemapaketteja opettajille ja kouluille. **Digizen** www.digizen.org **Insafe** www.saferInternet.org Osittain Euroopan unionin rahoittama Insafe on eurooppalainen Safer Internet Centre verkosto, joka edistää turvallista ja vastuullista Internetin ja mobiililaitteiden käyttöä nuorten keskuudessa. Se tarjoaa laajan valikoiman materiaaleja ja tietolähteitä useilla eri kielillä. Jokaisella jäsenmaalla on oma **Safer Internet Awareness Centre.** On mahdollista hyödyntää myös muiden maiden (esimerkiksi englannin- tai ruotsinkielisiä) Safer Internet Awareness Centre-aineistoja. **Euroopan komissio** "Eurooppalainen strategia Internetin parantamiseksi lasten näkökulmasta", saatavana useilla eri kielillä: http://ec.europa.eu/information_society/activities/sip/policy/index_en.htm **Teach today** www.teachtoday.eu/ Teachtoday-sivusto tarjoaa opettajille, rehtoreille ja muille koulun työntekijöille tietoa ja neuvoja uuden tekniikan myönteiseen, vastuulliseen ja turvalliseen hyödyntämiseen. Sivustolla olevien tapausesimerkkien avulla kouluttajat voivat herättää keskustelua osallistujien kohtaamista todellisista ongelmista kouluissa. www.teachtoday.eu/en/Case-studies.aspx
Arviointivaihtoehdot	• Jaa hyödyllinen linkki tai opetusmenetelmä twiittaamaalla siitä ryhmän Twitter-kanavalla. • Kirjoita merkintä oppimisblogiin.

Moduulin jälkeiset jatkotoimenpiteet	Ei ole.
Vaihtoehtoiset tavat toteuttaa moduuli	Ei ole.
Toteuttamisvaihtoehdot kansallisella/paikallisella tasolla	Tämä moduuli voidaan toteuttaa kansallisella/paikallisella tasolla.
Tehtävä 8.1:	**Ei harmaita alueita?**
Kesto	10 min
Tavoitteet	• Piristää ja virkistää ryhmää. • Herättää kevyempää keskustelua digitaaliseen turvallisuuteen liittyvistä kysymyksistä. • Auttaa ymmärtämään, että eri taustoista ja kulttuureista tulevat ihmiset lähestyvät digitaalisen turvallisuuden kysymyksiä eri tavoin.
Kuvaus	Tämä on hyvin lyhyt lämmittelytehtävä (kesto enintään 10 minuuttia) moduulin 8 aluksi. Siinä käytetään materiaalia eS 8.1 Ei harmaita alueita? – lämmittely pptx. Ainoa sääntö on, että osallistujien täytyy ottaa kantaa ja päättää, kummalle puolelle viivaa he siirtyvät; keskelle ei saa jäädä. Kouluttaja kertoo osallistujille, että esitetyt väittämät ovat yleisluonteisia, mutta huvin vuoksi osallistujien tulee päättää, ovatko he samaa vai eri mieltä seuraavista kolmesta väittämästä. Kouluttaja pitää tunnelman kevyenä ja temmon nopeana. Kouluttaja tulostaa diat 6 & 7 ennen lämmittelytehtävää. 1. Kouluttaja asettaa diojen 6 & 7 tulosteet vierekkäin viivan kummallekin puolelle. (Viiva voi olla todellinen tai kuvitteellinen. Tehtävässä käytetyn tilan tulisi olla pieni ja ahdas, jolloin osallistujien täytyy liikkua toistensa ympärillä, kun he päättävät kantansa). 2. Kun jokainen osallistuja on siirtynyt nopeasti asemiinsa, kouluttaja pyytää yhtä ihmistä kummaltakin puolelta perustelemaan kantansa. 3. Kouluttaja siirtyy seuraavaan diaan ja toistaa vaiheen 3, kunnes pääsee loppuun. 4. Kouluttaja päättää tehtävän kysymällä, liittyykö digitaalisen turvallisuuden kysymyksiin harmaita alueita. Onko kysymyksiin vain yksi oikea tai väärä vastaus? Entä ratkaisut? Onko vain yksi oikea ratkaisu?
Tehtävä 8.2	**Omat oppilaat, Internet-turvallisuuden teemapäivä ja vertaismentorointi**
Kesto	35 min
Tavoitteet	• Rohkaista koulun oppilaita käyttämään tieto- ja viestintätekniikkaa aktiivisesti myönteisiin tarkoituksiin. • Osallistaa oppilaat aktiivisiksi digikansalaisiksi. • Järjestää koko koulun digitaalisen turvallisuuden hanke Internet-turvallisuuden teemapäivänä.

	• Tarkastella digitaalisen turvallisuuden vertaisopetuksen hyötyjä ja mahdollisuuksia. • Kannustaa kouluja siihen, että oppilaat muodostaisivat niissä digitaalisen turvallisuuden nuorisopaneeleja.
Kuvaus	**Tehtävä** Kouluttaja pyytää osallistujia menemään sivustolle www.saferinternetday.org ja perehtymään siellä oleviin aineistoihin. Ryhmä keskustelee koko koulun teemapäivän, kuten Internet-turvallisuuden teemapäivän, tehosta ja vaikutuksesta. Osallistujat jakavat joitain esimerkkejä vertaisopetuksen hyvistä käytännöistä, Internet-turvallisuuden teemapäivään liittyvistä projekteista ja PanEU-nuorisopaneelin videoista. **Tehtävä** Kouluttaja pyytää osallistujia perehtymään seuraaviin materiaaleihin: www.beatbullying.org/about_this_site/ ja www.beatbullying.org/parents-and-carers/in-school/ . CyberMentors.org.uk on uusi digitaalisen ajan palvelu: perinteinen mentorointijärjestelmä, joka toteutetaan verkkoyhteisöpalvelun kautta. 11 - 25-vuotiaita nuoria koulutetaan virtuaalimentoreiksi kouluissa ja verkossa, jotta he voivat tukea ikätovereitaan. Ryhmä voi tutustua myös sivustoon The Web We Want www.webwewant.eu ja muihin aineistoihin, joita voi käyttää vertaisopetuksessa. Kouluttaja näyttää myös Norjan esimerkin oppilaista digitaalisen turvallisuuden lähettiläinä, materiaali eS 8.2a You Decide – vertaismentorointi - vanhemmat yläkoulun oppilaat opettavat nuoremmilleen digitaalista turvallisuutta You Decide -projektin puitteissa. Kouluttaja näyttää joitain palkittuja norjalaisia videoita ja tuntisuunnitelmia www.dubestemmer.no/en/Films/#content , esim. video "Maria". Kouluttaja korostaa, että kun nuorille annetaan työkalut ja vapautta, he voivat saada aikaan hyvin luovia tuotoksia.
Tehtävä 8.3	**Vanhempien osallistaminen**
Kesto	35 min
Tavoitteet	• Auttaa vanhempia tukemaan koulun digitaalisen turvallisuuden ohjelman tavoitteita. • Ymmärtää, kuinka osallistaa vanhemmat koulun digitaalisen turvallisuuden ohjelmaan. • Tehdä yhteistyötä vanhempien kanssa, jotta he pystyvät opettamaan lapsille turvallista ja vastuullista verkkokäyttäytymistä.
Kuvaus	Tutkimuksissa (EU Kids Online, Byron...) tulee jatkuvasti esiin se, että vanhemmat tarvitsevat koulun apua lasten tukemisessa ja verkkokäyttäytymisen opettamisessa. Katso videoita perheiden osallistamisesta osoitteessa: www.commonsensemedia.org/blog/common-sense-media-debuts-1-to-1-essentials

	Tehtävä Jokainen osallistuja avaa oman maansa Safer Internet Awareness Centre - verkkosivun ja perehtyy erilaisiin hankkeisiin ja tapoihin, joilla vanhempia tuetaan ja osallistetaan digitaalisen turvallisuuden kysymyksissä. Osallistujat raportoivat löytämistään hankkeista ja tavoista ja kouluttaja listaa ne kosketustaululle. Sen jälkeen osallistujat tutustuvat samalla tavoin Insafe-verkoston, Learning Resource Exchange -portaalin ja muiden tahojen vanhemmille tarkoitettuihin aineistoihin. Lisää tietoja: www.commonsensemedia.org/educators/parent-media-education **Keskustelua** • Kuinka vanhemmat tulee ottaa mukaan koulun digitaalisen turvallisuuden ohjelmaan, jotta halutut tulokset saavutetaan. • Kuinka voimme varmistaa, että vanhemmat ymmärtävät tietojärjestelmien käyttöehdot jne.? • Mitä koulu voi tehdä auttaakseen vanhempia? • Kuinka koulu voi ottaa vanhemmat mukaan toimintaan?
Tehtävä 8.4	**Asteittain etenevä koko koulun digitaalisen turvallisuuden opetussuunnitelma**
Kesto	35 min
Tavoitteet	• Laatia omalle koululle sopiva, asteittain etenevä digitaalisen turvallisuuden opetussuunnitelma. • Ymmärtää, kuinka koko koulun asteittain etenevä opetussuunnitelma on keskeinen osa koulun digitaalisen turvallisuuden ohjelmaa
Kuvaus	**Tehtävä** Jokaiselle osallistujalle annetaan post-it-lappu. Lappu kiinnitetään siihen vuosiluokan opetussuunnitelmaehdotukseen, joka on heidän mielestään kattava, helppo toteuttaa ja porrastettavissa. Opettajina haluamme hyödyntää Internetiä oppimisessa ja samalla välittää turvallisuustaitoja ja rohkaista kriittiseen ajatteluun ja eettiseen käyttäytymiseen. **Keskustelua** • Mihin opetussuunnitelmaan kiinnitettiin eniten post-it-lappuja? Miksi se oli mielestäsi suosituin? • Mihin riskeihin kyseisessä opetussuunnitelmassa puututaan? Käsitelläänkö siinä a) Turvallisuutta ja hyvinvointia, b) Digitaalista lukutaitoa ja c) Digikansalaisuutta? • Mitä vuorovaikutteisia digitaalisia oppimismahdollisuuksia suunnitelmaan sisältyy? • Mihin oppiaineisiin se on sisällytetty? Kuka opettaa? • Miksi digitaalisen turvallisuuden opetussuunnitelman pitäisi olla asteittain

	etenevä? Otetaanko siinä vanhemmat huomioon? **Tehtävä** Osallistujat avaavat verkkoversion materiaalista eS 7.4 Ehdotus oppiainerajat ylittäväksi koko koulun digitaalisen turvallisuuden opetussuunnitelmaksi (doc) [**Huomaa, että 7.4 käytetään uudestaan**] ja kirjaavat ylös opetussuunnitelmaan liittyviä ideoita, linkkejä ja aineistoja, joita he haluaisivat käyttää kouluissaan.
Kahvitauko	15 min
Tehtävä 8.5	**Kuinka kehittää digitaalista turvallisuutta omassa koulussa?**
Kesto	35 min
Tavoitteet	• Saada digitaalisen turvallisuuden kehittämistyö käyntiin kouluissa. • Kertoa digitaaliseen turvallisuuteen liittyvistä kysymyksistä kollegoille koulussa. • Keskustella digitaalisen turvallisuuden ohjelman tarpeesta muiden kollegojen kanssa koululla. • Perustaa kouluun digitaalisen turvallisuuden työryhmä, joka valmistelee digitaalisen turvallisuuden ohjelmaa. • Parantaa koulun sisäistä jatkokoulutusta digitaalisen turvallisuuden asioissa.
Kuvaus	Kouluttaja esittää materiaalin eS 8.5 Digitaalisen turvallisuuden vieminen kouluihin pptx **@ Dia 3** Edellisessä tehtävässä tarkasteltiin digitaalisen turvallisuuden opetussuunnitelman kolmea osa-aluetta, jotka ovat Turvallisuus ja hyvinvointi, Digitaalinen lukutaito ja Digikansalaisuus. Ehdotus digitaalisen opetussuunnitelman rungoksi on laadittu ja se on valmis esiteltäväksi kollegoille koulussa. (Mutta miten esittely kannattaa tehdä?) Digitaalisen turvallisuuden ja kurssilla saadun tiedon esittelyyn rehtorille ja muulle henkilökunnalle tarvitaan suunnitelma. **@ Dia 4** Kouluttaja näyttää dian ja selittää suunnitelman rakenteen samalla kun jakaa materiaalin eS 8.5a Esimerkki – Digitaalisen turvallisuuden kehittäminen kouluissa. Aluksi jokaisen osallistujan täytyy määrittää, millaista digitaalisen turvallisuuden ohjausta heidän koulussaan jo on: kuvaisivatko he koulunsa digitaalisen turvallisuuden ohjelmaa alkuvaiheessa olevaksi, keskitasoiseksi vai edistyneeksi? Esimerkkisuunnitelman koulu on alkuvaiheessa. Osallistujien tulee muokata suunnitelmansa omalle koululleen sopivaksi. **Keskustelua** • Kouluttaja pyytää osallistujia kertomaan, mistä tehtävien toteuttamistavoista he pitivät kurssilla, ja mitä niistä he voisivat käyttää esitellessään digitaalista turvallisuutta kollegoilleen koulussa.

	• Olisiko sopiva tapa esimerkiksi videot, viiden minuutin Teachmeet-tyyliset tuokiot henkilökunnan kokousten yhteydessä, käytännön workshopit, oppimisblogi, virtuaalisen oppimisympäristön tai Padletin käyttö henkilökunnan kokouksissa tai moraalikompassi? Kouluttaja pyytää osallistujilta ehdotuksia. **Tehtävä** Kouluttaja jakaa osallistujille materiaalin eS 8.5b Digitaalisen turvallisuuden kehittäminen kouluissa – pohja ja pyytää heitä täyttämään sen. Kouluttaja pyytää yhtä tai kahta osallistujaa kertomaan suunnitelmastaan ja ideoistaan.
Tehtävä 8.6	**Oppimisen pohdintaa**
Kesto	15 min
Tavoitteet	• Tehdä yhteenveto osallistujien päivän aikana oppimista asioista ja siitä, miten he aikovat ryhtyä soveltamaan opittua käytäntöön kouluissa. • Kertoa muille, kuinka osallistujat aikovat osallistaa vanhemmat koulunsa digitaalisen turvallisuuden ohjelmaan.
Kuvaus	Osallistujat jakavat ehdotuksensa aineistoiksi ja keskustelevat siitä, kuinka he kehittävät digitaalisen turvallisuuden taitoja ja osaamista omissa kouluissaan kurssin jälkeen.

Moduuli 8: KURSSIN TUKIMATERIAALIT

Kurssi/Moduuli/Tehtävä	**Kurssin tukimateriaalit**
eS 8.1	Ei harmaita alueita? – lämmittely (pptx)
eS 8.5	Digitaalisen turvallisuuden kehittäminen kouluissa (pptx)
eS 8.5a	Esimerkkisuunnitelma – digitaalisen turvallisuuden kehittäminen kouluissa (PDF)[moniste]
eS 8.5b	Digitaalisen turvallisuuden kehittäminen kouluissa – pohja (doc)[moniste]
Tukimateriaalia	Nämä aineistot voi lisätä kurssin verkkoalueelle:
eS 8.2a	You Decide – vertaismentorointi – käännös (PDF)
eS 7.4 (käytetään uudelleen kohdassa eS 8.4)	Ehdotus oppiainerajat ylittäväksi koulun digitaalisen turvallisuuden opetussuunnitelmaksi (doc)

Kouluttajan käsikirja ja tukimateriaalit

Kurssi:

Digitaalinen turvallisuus: TURVALLISEMPI KOULU JA LUOKKAYMPÄRISTÖ

Moduuli 9: Koko koulun digitaalisen turvallisuuden ohjelma

(eS 9.0)

eS 9.0: Koko koulun digitaalisen turvallisuuden ohjelma

CPDLab-kurssi	**Digitaalinen turvallisuus: Digitaalisen turvallisuuden parantaminen kouluissa**
Moduulin numero	**eS 9.0**
Moduulin nimi	**Koko koulun digitaalisen turvallisuuden ohjelma**
Vaatimukset moduulin suorittamiseen	• Osallistujien tulee olla kiinnostuneita digitaalisen turvallisuuden suunnittelusta koko koulun tasolla ja digitaalisen turvallisuuden sisällyttämisestä koulun opetussuunnitelmaan. • **HUOM:** EU:n eSafety Label -hankkeen henkilökunnalle tulee ilmoittaa, että osallistujaryhmä saattaa rekisteröityä eSafety Label-projektiin. Osallistujilla pitää olla mahdollisuus käyttää sähköpostiosoitetta, jota tarvitaan EU eSafety Label -työkalun asentamiseen ja käyttämiseen. • Osallistujilla tulee olla perustaidot tieto- ja viestintätekniikan käytössä ja kiinnostus digitaalisen teknologian ja Internetin turvalliseen käyttämiseen opetuksessa ja oppimisessa. • Osallistujien tulisi tuntea jonkin verran sosiaalisen median palveluita, erityisesti vuorovaikutteisia sosiaalisen median pedagogisia työkaluja, kuten blogit, eTwinning ja virtuaaliset oppimisympäristöt, sekä kyseisten palvelujen toimintaa ja sitä, miten niitä voidaan käyttää tehostamaan opetusta ja oppimista. • Osallistujien tulee lisäksi perustaa sosiaalinen kirjanmerkkitili ennen kurssia. Kurssille osallistuvien **rehtorien ja TVT-koordinaattorien** tulisi tehdä ennen kurssia koulunsa digitaalisen turvallisuuden ohjeistuksen minikartoitus ja seuraava kurssin/moduulin ennakkotehtävä: Lue asiakirja eS 10.1x - Yhteenveto tutkimustuloksista. Se tarjoaa yleiskäsityksen tämänhetkisistä digitaaliseen turvallisuuteen liittyvistä kysymyksistä. • Mitä näistä kysymyksistä ja ongelmista on käsitelty omassa koulussasi? • Kuinka näitä kysymyksiä voi hyödyntää koko koulun digitaalisen turvallisuuden ohjelman hahmottelussa? • Kuinka digitaalisen turvallisuuden kysymykset otetaan huomioon opetuksessa ja oppimisessa luokkaympäristössä? • Onko koulullasi koko koulun kattava, asteittain etenevä digitaalisen turvallisuuden opetussuunnitelma? • Mitä digitaaliseen turvallisuuteen liittyviä ohjeita koulullasi on?

	• Milloin ne on viimeksi tarkistettu ja päivitetty? Ovatko käyttöehdot ja ohjeet helposti ymmärrettäviä oppilaille? • Järjestetäänkö henkilökunnalle koulun sisäistä koulutusta ja työpajoja koulun tieto- ja viestintätekniikan turvallisesta ja asianmukaisesta opetus- ja oppimiskäytöstä?
Kesto	3 tuntia
Kurssipaikka ja moduulin rakenne	• Tämä moduuli järjestetään lähiopetuksena. • Osallistujia kehotetaan ottamaan mukaan oma kannettava tietokoneensa, sillä moduulin aikana kokeillaan opetettavia asioita käytännössä. • Lisäksi moduuliin kuuluu tehtäviä, keskustelua, ryhmätöitä ja pohdintaa.
Tarvittavat tilat ja tilajärjestelyt	• Kouluttaja tarvitsee käyttöönsä kosketustaulun, tietokoneen ja langattoman verkon. • Jokainen osallistuja tarvitsee käyttöönsä tietokoneen, jossa on Internet-yhteys. • Tiloissa tulisi olla tarpeeksi virtapistokkeita kannettaville tietokoneille. • Lisäksi osallistujat tarvitsevat tiloja, joihin hajaantua työskentelemään 3–5 hengen pienryhmissä.
Moduulin yleiskuvaus	Tätä moduulia voi muokata sopivaksi joko opettajille, jotka suorittavat koko kurssin (Ryhmä O), tai rehtoreille (Ryhmä R) ja koulunjohtajille, jotka suorittavat ainoastaan moduulit 9 ja 10. Opettajien kohdalla kouluttaja kertaa lyhyesti parhaat käytännöt. Rehtorien kohdalla kouluttaja esittelee koko koulun digitaalisen turvallisuuden ohjelman parhaana käytäntönä. Kouluttaja esittelee lyhyesti eurooppalaisen eSafety Label -projektin ja antaa osallistujien tutustua sivustoon www.esafetylabel.eu . Osallistujat liittyvät eSafety-portaaliin. Halutessaan osallistujat voivat luoda koulun profiilin (School Profile). Profiilia tarvitaan, jos osallistujat haluavat täyttää arviointikyselyn (Assessment Quiz). (Monet tekevät kyselyn mieluummin vasta kurssin jälkeen, koska kyselyn täyttämisessä avustaa koulun digitaalisen turvallisuuden työryhmä. Työryhmät muodostetaan kouluissa vasta kurssin jälkeen.) Kouluttajien tulee mainita osallistujille, että koulu voi tehdä arviointikyselyn vain kerran 18 kuukauden jakson aikana. Osallistujat keskustelevat siitä, kuinka digitaaliseen turvallisuuteen liittyvät ongelmatapaukset raportoidaan, kuinka niihin puututaan ja kuinka ne käsitellään heidän kouluissaan. Osallistujat keskustelevat siitä, mikä on sopimatonta ja mikä laitonta käyttöä, ja kuinka nämä vaativat erilaista reagointia. He keskustelevat kouluissa tarvittavista erilaisista toimintaohjeista, mukaan lukien henkilökunnan ohjeistus.

	Ryhmä keskustelee siitä, miten Internetin mobiilikäyttö vaikuttaa toimintaan koululla ja luokissa, sekä oman teknologian käyttöön liittyvien päätösten vaikutuksista. Osallistujat, jotka eivät tee eSafety Label -projektin arviointikyselyä (koska he haluavat perustaa koulun digitaalisen turvallisuuden työryhmän takaisin koululle palattuaan) voivat keskustella esimerkkikoulun digitaalisen turvallisuuden toimintasuunnitelmasta ja arvioida koulun opetussuunnitelmaa, toimintaohjeita ja tieto- ja viestintäteknistä infrastruktuuria. Arviointikyselyn tehneet osallistujat arvioivat oman koulunsa digitaalisen turvallisuuden ohjelmaa koulun opetussuunnitelman, toimintaohjeiden ja tieto- ja viestintäteknisen infrastruktuurin näkökulmasta. Kaikki osallistujat laativat toteuttamissuunnitelman eSafety Label -toimintasuunnitelmansa tai esimerkkitoimintasuunnitelman ehdotusten pohjalta.
Moduulin tavoitteet	• tunnistaa tarve koko koulun asteittain etenevälle digitaalisen turvallisuuden opetussuunnitelmalle • välittää tietoa eurooppalaisesta eSafety Label -projektista ja sen tuloksista • tarjota osallistujille mahdollisuus kartoittaa koulujensa digitaalisen turvallisuuden taso • laatia toteuttamissuunnitelma, jossa nimetään keskeisimmät tekijät koulun digitaalisen turvallisuuden edistämiseksi.
Taitojen ja osaamisen karttuminen tässä moduulissa	Osallistujat oppivat • soveltamaan käytännöllisiä työkaluja oman koulunsa itsearviointiin • arvioimaan oman koulunsa digitaalisen turvallisuuden ohjeistusta ja • tunnistamaan kehitystarpeita • arvioimaan oman koulunsa digitaalisen turvallisuuden ohjelmaa • suunnittelemaan digitaaliseen turvallisuuteen liittyvien toimintaohjeiden ja käytäntöjen kehittämistä • arvioimaan, kuinka digitaaliseen turvallisuuteen liittyvät asiat on järjestetty heidän omassa koulussaan • pohtimaan koko koulun asteittain etenevän digitaalisen turvallisuuden opetussuunnitelman tarvetta.
Tarvittavat materiaalit ja välineet	Pääsy kurssin verkkosisältöalueelle ja keskustelufoorumiin **HUOM.:** Jokaisella osallistujalla, joka haluaa rekisteröityä ja liittyä EU:n eSafety Label -projektiin ja saada eSafety Label -tunnustuksen, täytyy olla pääsyoikeudet. ESafety Label -projektin henkilökunnalle täytyy ilmoittaa, että 20–30 uutta koulua saattaa tarvita eSafety Label -tunnustuksen ja tukea koulutuspäivänä. **HUOM.:** Osallistujilla pitää olla mahdollisuus käyttää sähköpostiosoitetta,

	jota tarvitaan EU eSafety Label -työkalun asentamiseen ja käyttämiseen. Monisteet eS 9.3a – eS.9.3b
Vaatimukset kouluttajalle	Kouluttajan tulee tuntea eSafety Label -projekti ja sen verkkoportaalin sisältö. Kouluttajan tulee ymmärtää koulumaailman strategista suunnittelua ja tietää, millaisia asioita koulun digitaalisen turvallisuuden ohjelman täytyisi sisältää. Kouluttajalla tulee olla syvällinen ja monipuolinen tietämys digitaalisesta lukutaidosta, digitaaliseen turvallisuuteen liittyvistä kysymyksistä ja digitaalisen turvallisuuden opetussuunnitelmista. Kouluttajan tulee tuntea EU:n politiikka, joka tähtää Internetin parantamiseen lasten ja nuorten näkökulmasta, Insafen materiaalit ja palvelut sekä paikallisen Safer Internet Centren materiaalit ja kansainvälinen digitaalisen turvallisuuden opetussuunnitelma. Kouluttajan tulee tutustua kurssin verkkoalueeseen ja kaikkiin kurssin tukimateriaaleihin, jotka on lueteltu jokaisen moduulin lopussa. Jokainen materiaali on luetteloitu kurssin, moduulin ja tehtävän mukaan, esim. eS 1.1 "Ihmisbingo digikansalaisille" Kouluttajan tulee käyttää sosiaalista kirjanmerkkipalvelua (esim. www.delicious.com tai Diigo www.diigo.com), jonne tallennetaan digitaaliseen turvallisuuteen liittyviä linkkejä ja materiaaleja. Kouluttajan tulee myös kannustaa osallistujia luomaan oma käyttäjätili kurssilla jaettujen linkkien ja verkkomateriaalien hallinnoimiseksi. Kouluttajan tulee perustaa oppimispäiväkirja ja antaa sen käyttäjätunnukset ja salasana osallistujille. Sen lisäksi kouluttajan täytyy osata käyttää ryhmätyösovelluksia, blogeja, etherpadia, padletia ja vastaavia sovelluksia.
Lähdeaineistoja ja materiaaleja kouluttajille	**EU:n eSafety Label -työkalu itsearviointiin** www.eSafetylabel.eu Asiakirjat eS 9.2b ja c: Esittely -eSafety Label pdf ja Raportti -eSafety Labelin kehittäminen pdf ovat saatavilla kouluttajan tukimateriaaleissa. **360 asteen arviointi - materiaali** (Britannia) www.360safe.org.uk Työkalu kouluille digitaalisen turvallisuuden tason itsearviointiin. **Online Compass** www.onlinecompass.org.uk Itsearviointityökalu verkossa, tarkoitettu nuorisoryhmille ja järjestöille, jotka tekevät töitä lasten ja nuorten kanssa. **Insafe** www.saferInternet.org Osittain Euroopan unionin rahoittama Insafe on eurooppalainen Safer Internet Centre -verkosto, joka edistää turvallista ja vastuullista Internetin ja mobiililaitteiden käyttöä nuorten keskuudessa. Se

	tarjoaa laajan valikoiman materiaaleja ja tietolähteitä useilla eri kielillä. Jokaisella jäsenmaalla on oma **Safer Internet Awareness Centre.** On mahdollista hyödyntää myös muiden maiden (esimerkiksi englannin- tai ruotsinkielisiä) Safer Internet Awareness Centre-aineistoja. **Safer Internet Day** (SID) www.saferInternetday.org Helmikuun toisena tiistaina vietetään kouluissa vuosittain kansainvälistä Internet-turvallisuuden teemapäivää (Safer Internet Day). EU:n hanke tarjoaa materiaaleja, oppituntisuunnitelmia ja teemapaketteja opettajille ja kouluille. **Euroopan komissio** "Eurooppalainen strategia Internetin parantamiseksi lasten näkökulmasta", saatavana useilla eri kielillä: http://ec.europa.eu/information_society/activities/sip/policy/index_en.htm **Teach today** www.teachtoday.eu/ Teachtoday-sivusto tarjoaa opettajille, rehtoreille ja muille koulun työntekijöille tietoa ja neuvoja uuden tekniikan myönteiseen, vastuulliseen ja turvalliseen hyödyntämiseen. Sivustolla olevien tapausesimerkkien avulla kouluttajat voivat herättää keskustelua osallistujien kohtaamista todellisista ongelmista kouluissa. www.teachtoday.eu/en/Case-studies.aspx
Arviointivaihtoehdot	• Osallistujat kirjoittavat merkinnän oppimisblogiin. • Osallistujat jakavat ryhmälle linkin johonkin videoon.
Moduulin jälkeiset jatkotoimenpiteet	• Digitaalinen turvallisuus henkilökunnan kokouksen asialistalle. • Koulun digitaalisen turvallisuuden työryhmän perustaminen digitaalisen turvallisuuden ohjelman toteuttamista varten. • Toimintasuunnitelman keskeisten asiakohtien toteuttaminen • Digitaalisen turvallisuuden täydennyskoulutuksen edistäminen koulun sisäisen koulutuksen kautta.
Vaihtoehtoiset tavat toteuttaa moduuli	Tämä moduuli voidaan järjestää • **Ryhmälle O:** Opettajat, jotka suorittavat kaikki 10 moduulia • Ryhmälle **R: Rehtorit** ja TVT-koordinaattorin tehtäviä hoitavat opettajat, jotka suorittavat moduulit 9 ja 10. Jokaisen tehtävän kohdalla on selitetty erikseen, kuinka **Ryhmä O** ja **Ryhmä R** voivat suorittaa tehtävän.

Toteuttamisvaihtoehdot kansallisella/paikallisella tasolla	Osallistujat saattavat tuntea paikallisia digitaalisen turvallisuuden itsearviointiin tarkoitettuja työkaluja, joita voidaan käyttää. Osallistujilla tulisi olla pääsy näihin työkaluihin. Jos heillä on kattavat tiedot koulun tieto- ja viestintäteknisestä infrastruktuurista, käytännöistä ja opetussuunnitelmasta, he voivat syöttää tiedot työkaluun ja asettaa sitten koulun digitaalisen turvallisuuden ohjeistukseen tehtävät muutokset tärkeysjärjestykseen. Monet osallistujat perustavat mieluummin koululle palattuaan koulun digitaalisen turvallisuuden työryhmän. Saatavilla on monia muitakin ilmaisia työkaluja digitaalisen turvallisuuden itsearviointia varten. Kouluttaja voi näyttää paikallisille osallistujille heidän omassa koulutusjärjestelmässään käytetyn työkalun, esim. 360safe tai The Online Compass (erityisesti nuorisoryhmille) Osallistujat voivat halutessaan valita työkalun, joka tuntuu heille sopivimmalta, ja aloittaa tietojen syöttämisen siihen.
Tehtävä 9.1	**Digitaalisen turvallisuuden ohjelman laatiminen – mitkä ovat parhaat käytännöt?**
Kesto	15 min
Tavoitteet	• Kurssin sisällön arviointi. • Digitaalisen turvallisuuden ja parhaiden käytäntöjen määrittely. • Ymmärryksen herättäminen siitä, että koulun digitaalisen turvallisuuden ohjelma on paras tapa tarjota turvallinen oppimisympäristö.
Kuvaus	**Ryhmä O:** Tämä on kertaustehtävä, joten se pidetään lyhyenä. **Ryhmä R:** Tämä on tärkeä yleiskatsaus, jossa esitellään tarve koko koulun digitaalisen turvallisuuden ohjelmalle. Kouluttaja näyttää materiaalin eS 9.1: Digitaalisen turvallisuuden ohjelma omalle koulullesi Digitaalisen turvallisuuden ohjelmien parhaat käytännöt, kolme toisiinsa liittyvää osatekijää, kolme osatekijää ("3Cs") – kolme erityyppistä riskiä (muokattu EU KidsOnline- ja Byron-diasta) Millaisia ongelmia kouluissa on digitaaliseen turvallisuuteen liittyen? Kuinka voimme luoda turvallisia oppimisympäristöjä, suojella lapsia ja nuoria epäasialliselta sisällöltä sekä samalla kannustaa opettajia käyttämään luokassa digitaalista teknologiaa opetustyökaluna ja osana oppimisympäristöä? Kuinka voimme tarjota oppilaille oppimismahdollisuuksia, jotka kannustavat turvalliseen yhteistoiminnallisten ja vuorovaikutteisten verkkotyökalujen käyttöön eri oppiaineissa? Digitaalinen turvallisuus täytyy sisällyttää osaksi koulun opetussuunnitelmaa. Opetussuunnitelman tulee sisältää seuraavat osa-alueet: henkilökohtainen turvallisuus, digitaalinen lukutaito ja digikansalaisuus. Tarvitaan helppokäyttöinen työkalu edistymisen itsearviointiin, esim. EU:n eSafety Label.

Tehtävä 9.2:	**eSafety Label – liittyminen yhteisöön**
Kesto	20 min
Tavoitteet	• Oppia tuntemaan eSafety Label -projekti ja sen kouluille tarjoamat palvelut. • Rekisteröidä oma koulu palveluun. • Perustaa koulun profiili. • Pyytää eSafety Label -tunnustusta.
Kuvaus	**Tiedoksi kouluttajalle** Osallistujat tarvitsevat sähköpostiosoitteen tätä tehtävää varten. Kouluttaja esittelee eSafety Label -projektin ja sen verkkoportaalin osoitteessa www.eSafetylabel.eu/. eSafety Label on kouluille tarkoitettu työkalu turvallisen verkon käytön tukemiseen ja eSafety-tunnustuksen saamiseen. eSafety Label on eurooppalaisten koulujen tukipalvelu. Sen on kehittänyt European Schoolnet -hanke yhteistyössä alan keskeisten toimijoiden ja opetusministeriöiden kanssa. eSafety Label tulee olemaan itsenäinen järjestelmä, jonka puitteissa koulut voivat hakea eSafety-tunnustusta ja saada tukea ja materiaaleja. Kouluttaja kertoo, kuinka eSafety Labelin itsearviointityökalua käytetään, ohjeet materiaalissa eS 9.2a eSafety Label – arviointityökalu (pptx) Ryhmä keskustelee, kuinka eSafety Label -työkalu auttaa tunnistamaan kehittämiskohteita, ja kouluttaja jakaa tietosivuja, jotka auttavat seuraavissa asioissa: • käytäntöjen laatiminen esiin nousevia kysymyksiä varten, käytäntöjen arviointi • kuinka sisällyttää digitaalisen turvallisuuden opetus opetussuunnitelmaan • kuinka arvioida tieto- ja viestintäteknisen infrastruktuurin turvallisuutta ja menettelytapoja. **Tehtävä** Osallistujat tutustuvat www.eSafetylabel.eu -portaaliin ja luovat palveluun tilin ja koulun profiilin napsauttamalla **Join the Community** -kuvaketta. Sen jälkeen he odottavat rekisteröitymisviestiä sähköpostiinsa. Kun viesti on tullut, he voivat osallistua tehtävään 9.4.
Tehtävä 9.3:	**Omassa koulussani... Ongelmatapausten käsittely**
Kesto	1 h
Tavoitteet	• Jakaa strategioita digitaaliseen turvallisuuteen liittyvien ongelmien käsittelyyn kouluissa. • Pohtia, kuinka luoda parempia toimintaohjeita. • Tunnistaa ero laittomaan ja sopimattomaan tai vaaralliseen käyt-

	töön liittyvien tapausten välillä. • Sisällyttää toimintaohjeisiin raportointijärjestelmät.
Kuvaus	**Keskustelu akvaariomenetelmällä** • Millaiset ovat omat selviytymistaitomme opettajan tai rehtorin roolissa? • Onko oma riskienhallintamme kunnossa? Jokainen ryhmä keskittyy ongelmatapausten käsittelyyn ja hallintaan ja keskustelee, kuinka kyseiset tilanteet käsiteltäisiin heidän koulussaan, kuinka niihin puututaan, kuinka niitä voidaan ehkäistä tai estää tapahtumasta. Opettajana toimivat osallistujat, jotka kuuluvat **Ryhmä O:hon**. Kouluttaja kertoo ryhmälle ongelmatapauksen, josta ryhmä keskustelee. (Kouluttajan tulisi käyttää esimerkkinä kouluissa oikeasti tapahtuneita ongelmatilanteita.) • Ryhmä O1 keskustelee opettajien ongelmatilanteista.Toinen ryhmä tarkkailee keskustelua ja tekee muistiinpanoja, mutta kommentoi vasta keskustelun lopuksi. Ryhmät vaihtavat paikkoja. • Ryhmä O2 keskustelee oppilaiden ongelmatilanteista.Toinen ryhmä tarkkailee keskustelua ja tekee muistiinpanoja, mutta kommentoi vasta keskustelun lopuksi. Rehtorina toimivat osallistujat, jotka kuuluvat **Ryhmä R:ään** Kouluttaja kertoo ryhmälle ongelmatapauksen, josta ryhmä keskustelee. (Kouluttajan tulisi käyttää esimerkkinä kouluissa oikeasti tapahtuneita ongelmatilanteita) • Ryhmä R1 keskustelee lainopillisista ja tietosuojaan liittyvistä kysymyksistä, esim. siitä, miten koulu kannustaa kaikkia käyttämään tieto- ja viestintätekniikkaa ja jakamaan aineistoja. Opettajat käyttävät oppilaiden kanssa omia Dropbox-tilejään. Kun opettaja lähtee koululta toiseen työpaikkaan, kuka omistaa pilvessä olevat tiedot? Kenellä on pääsy niihin? Toinen ryhmä tarkkailee keskustelua ja tekee muistiinpanoja, mutta kommentoi vasta keskustelun lopuksi. Ryhmät vaihtavat paikkoja. • Ryhmä R2 keskustelee toimintaohjeista ja henkilökuntaa ja oppilaita koskevista turvallisuuskysymyksistä.Toinen ryhmä tarkkailee keskustelua ja tekee muistiinpanoja, mutta kommentoi vasta keskustelun lopuksi. Kouluttaja johtaa keskustelua koko ryhmän kesken. Onko osallistujilla muita esimerkkejä kohtaamistaan ongelmatapauksista? Mitä menettelytapoja heidän kouluissaan on vastaavanlaisten tapausten käsittelemiseksi? Onko koulussa käytössä tietojärjestelmien käyttöehdot henkilöstölle? Millaista tukea osallistujien kouluissa tai kotimaissa on tarjolla opettajille tai oppilaille?

Kouluttaja voi myös jakaa otteita Ofstedin asiakirjasta: eS 10.2c Hyvien ja riittämättömien käytäntöjen tunnusmerkkejä. www.ofsted.gov.uk/resources/safe-use-of-new-technologies, jossa arvioidaan Britannian kouluja. Asiakirjassa käsitellään hyviä ja erinomaisia digitaalisen turvallisuuden käytäntöjä (sekä myös riittämättömiä toimintatapoja).

Riittämättömien käytäntöjen tunnusmerkkejä

- Henkilökohtaiset tiedot ovat usein suojaamattomia ja/tai niitä lähetetään koulun alueelta ilman salausta.
- Salasanojen suojaus on tehotonta, esimerkiksi salasanoja jaetaan tai ne ovat yhteisiä kaikkien paitsi nuorimpien lasten osalta.
- Toimintaohjeet ovat yleisluontoisia ja niitä ei päivitetä.
- Opetussuunnitelmaan ei sisälly asteittain etenevää, suunnitelmallista digitaalisen turvallisuuden opetusta; koulussa järjestetään esimerkiksi vain vuosittainen teemapäivä.
- Internetin käyttöä ei valvota tai suodattimia ei ole käytössä.
- Henkilökunnalle ei tarjota koulutusta.
- Oppilaat eivät tiedä, kuinka ilmoittaa ongelmista.

Kouluttaja varaa osallistujille aikaa keskustella näistä väitteistä ja pohtia näkemyksiään.

Tehtävä 2
Osallistujat perehtyvät Britanniassa tarjottavaan tukeen ja palveluihin ja sitten oman maansa Safer Internet Awareness Centren palveluihin sivuston www.saferinternet.org kautta. Osallistujat tutustuvat lapsille ja nuorille suunnattuun neuvontapuhelimeen ja vihjepalveluun. Onko ammattilaisille olemassa neuvontapalvelua? Ammattiliittojen tukea? Muuta tukea? Kouluttaja näyttää ohjeita ammatillisuuden suojaamiseen osoitteessa: www.childnet.com/teachers-and-professionals/for-you-as-a-professional/professional-reputation

Kouluttaja pyytää osallistujia (**etenkin ryhmää R**) tutustumaan sivustoon ja miettimään miten osallistujat huomioivat ammatillisuuden suojaamisen omassa sosiaalisen median käytössään? Mitä olemme oppineet? Millä muilla tavoilla me voisimme suojautua riskeiltä? Onko osallistujien omassa maassa samantyyppistä ohjeistusta? Kouluttaja jakaa sivuston ja tallentaa sen kirjanmerkkeihin.

Tiedoksi kouluttajalle
Seuraava tehtävä (nro 3) koskettaa erityisesti Ryhmää R ja opinto-ohjaajia. Ryhmä O saattaa tutustua mieluummin Internet Watch Foundationin (IWF) sivustoon ja keskustella sitten pienryhmissä ja tehdä tehtäviä jaetun monisteen pohjalta: eS 9.3a Luonnos: digitaalisen turvallisuuden muistilista koululle

Tehtävä 3
Digitaaliseen turvallisuuteen liittyvät juridiset näkökohdat
Kouluttaja pyytää osallistujia avaamaan seuraavan sivuston:
www.iwf.org.uk/resources/best-practice-guide/frequently-asked-questions
Mieti Internetin, kuvien ja tekstien käyttöön liittyviä juridisia kysymyksiä, jotka voivat koskettaa koulua, ja erityisesti koulun verkon aikuisia käyttäjiä (opetushenkilökunta, huoltohenkilökunta, vieraskäyttäjät...).

esim. Organisaation toimintaohjeet, IWF

Kaikilla organisaatioilla tulisi olla selkeät toimintaohjeet siitä, miten hoidetaan ongelmatapaukset, joihin liittyy sopimattomia kuvia lapsista, mukaan lukien

- organisaation tarjoamien elektronisten laitteiden hyväksyttävä käyttö
- kuinka käsitellä tapaukset, jossa henkilökunnan hallusta löydetään sopimattomia kuvia lapsista
- miten toimitaan, jos löydetään sopimattomia kuvia lapsista.

Kouluttaja pyytää osallistujia luetteloimaan erityyppisiä juridisia kysymyksiä ja mahdollisia piileviä juridisia vaaroja, joita koulujen täytyy käsitellä tai joita koulut voivat kohdata: todennäköisiä vastauksia ovat tietosuoja, tekijänoikeuksien loukkaukset, häirintä, pornografia, seksuaalissävytteinen viestittely ja seksuaalirikokset, identiteettivarkaudet, omaisuusvarkaudet, kunnianloukkaus.

Tehtävä 4
(**Sekä Ryhmä O** että **R**) Osallistujat avaavat linkin
www.swgfl.org.uk/Staying-Safe/Creating-an-E-Safety-policy ja tarkastelevat joitain sivustolla olevia netikettipohjia.

Tehtävä 5
Löytävätkö osallistujat vastaavan sivuston omalla kielellään?

Esimerkki swgfl.org-sivuston netiketin muotoilusta: "Käyttäjät eivät saa vierailla Internet-sivustoilla tai tehdä, lähettää, ladata, laittaa verkkoon tai välittää materiaalia, huomautuksia, ehdotuksia tai kommentteja, joiden sisältöön liittyy tai joka on:

- pornografiaa (mukaan lukien lapsipornografia)
- minkäänlaisen syrjinnän levittämistä
- rotu- tai uskontovihan levittämistä
- laittomien tekojen edistämistä
- muuta tietoa, joka voi loukata kollegoja."

Entä **henkilökunnalle tarkoitetut Internetin käyttösäännöt**? Onko niitä olemassa?

	Onko osallistujien kouluissa selkeät toimintaohjeet sekä oppilaille että henkilökunnalle? Mitä niihin tulisi sisältyä? **Tehtävä 6** Kouluttaja kiinnittää osallistujien huomion erityisesti seuraavaan: Pohja **koulun henkilökohtaisten tietojen käsittelyn toimintaohjeille**. Onko niitä olemassa? Katkelma: "Kun kouluyhteisön jäsenet käsittelevät, käyttävät tai siirtävät henkilökohtaisia tietoja, heillä kaikilla on velvollisuus varoa, että niihin ei pääse käsiksi kukaan, jolla • ei ole lupaa käyttää tietoja, ja/tai • ei ole tarvetta käyttää tietoja. Tietomurroilla voi olla vakavia vaikutuksia niiden kohteeksi joutuneille henkilöille ja/tai laitoksille, sillä ne voivat tahrata koulun maineen ja johtaa kurinpitotoimiin, rikossyytteisiin ja sakkoihin koululle ja asianosaisille henkilöille. Erityisesti tietojen siirrossa on riski tietojen katoamiselle tai leviämiselle asiattomaan käyttöön. Kaikkien henkilöiden, joilla on pääsy henkilökohtaisiin tietoihin, täytyy tuntea ja ymmärtää nämä toimintaohjeet ja noudattaa niitä. Toimintaohjeet täyttävät asiaan liittyvän tietosuojalainsäädännön sekä säädösten ja ohjeistuksen vaatimukset." Ymmärtääkö koulun henkilökunta vastuunsa henkilökohtaisten tietojen käsittelyssä? Ymmärtävätkö he vastuunsa pilvipalveluiden käytössä? **Tehtävä 7** Ryhmä keskustelee osallistujien koulujen ilmoitusjärjestelmistä, mikäli ongelmatapauksia ilmenee. Ovatko ne tehokkaita ja selkeitä? Ryhmä keskustelee myös parhaista käytännöistä todisteiden suojaamiseksi. Kouluttaja pyytää osallistujia kertomaan esimerkkejä. Kuinka he käsittelevät tapauksia, joissa koulun järjestelmästä löytyy laitonta materiaalia vs. tapauksia, joissa koulun järjestelmästä löytyy sopimatonta materiaalia tai esiintyy sopimatonta käytöstä? Moniste eS 9.3b Käyttösääntöideoita mietittäväksi
Kahvitauko	**15 min**
Tehtävä 9.4	**Olemmeko valmiita omien laitteiden (BYOT) tai henkilökohtaiseen käyttöön annettujen laitteiden (1:1) käyttöön?**
Kesto	35 min
Tavoitteet	• Tunnistaa, kuinka omien laitteiden käyttö vaikuttaa jossakin muodossa jokaiseen kouluun. • Keskustella koulun digitaalisen turvallisuuden ohjelman tarpeesta, jotta voidaan hallita omien laitteiden käyttöä. • Keskustella, kuinka laatia parempia toimintaohjeita ja -tapoja

	omien laitteiden käyttöönottoon valmistautuessa. • Pohtia, kuinka omien laitteiden käyttö vaikuttaa tarpeeseen osallistaa vanhemmat entistä enemmän.
Kuvaus	Kouluttaja esittelee oman teknologian käyttöön tähtäävän BYOT-liikkeen eS 9.4 Olemmeko valmiita omien laitteiden (BYOT) tai henkilökohtaiseen käyttöön annettujen laitteiden (1:1) käyttöön? pptx ja näyttää CommonSense-Median www.commonsensemedia.org/educators/1to1 materiaalia, joka käsittelee henkilökohtaiseen käyttöön annettuja laitteita, myös videoita: **Mitä BYOT eli oman teknologian käyttö tarkoittaa** www.commonsensemedia.org/educators/1to1/phase1 **Tukea opettajille** www.commonsensemedia.org/videos/supporting-teachers **Vanhempien osallistaminen** www.commonsensemedia.org/videos/engaging-families **Digikansalaisuuteen kannustaminen** www.commonsensemedia.org/videos/encouraging-digital-citizenship **Tehtävä** **1** Moniste eS 9.4a Oman teknologian käyttö ja usein kysytyt kysymykset – vanhemmat ja oppilaat. Keskustelua: • Millaisia tieto- ja viestintäteknisen infrastruktuurin muutoksia, toimintaohjeiden laatimista ja opetussuunnitelman muutoksia osallistujien kouluissa vaadittaisiin ennen oman teknologian käyttöönottoa? • Millaista koulun sisäistä täydennyskoulutusta opettajille tarvitaan ennen kuin aloitetaan oman teknologian käyttö? • Voisiko materiaalia eS9.4a käyttää pohjana keskusteluissa henkilökunnan kanssa, kun osallistujat palaavat takaisin kouluihinsa? • Voisiko sitä käyttää jopa oman teknologian käyttöä koskevien usein kysyttyjen kysymysten ja vastausten laatimiseen opettajille?
Tehtävä 9.5	**Oman koulun digitaalisen turvallisuuden tason itsearviointi – eSafety Label -työkalun käyttäminen**
Kesto	30 min
Tavoitteet	• Oman koulun digitaalisen turvallisuuden ohjelman arviointi. • Opastus digitaalisen turvallisuuden ohjelman kehittämiseen ja parantamiseen.
Kuvaus	• Halutessaan osallistujat voivat tehdä eSafety Label -projektin arviointikyselyn.

	• Työkalu kehittää osallistujan oman koulun/organisaation digitaalisen turvallisuuden tarpeisiin perustuvan toimintasuunnitelman. • Työkalu luo toimintasuunnitelman lounastauon aikana.
Lounas	1 tunti

Moduuli 9: KURSSIN TUKIMATERIAALIT

Kurssi/Moduuli/Tehtävä	Kurssin tukimateriaalit
eS 9.1:	Digitaalisen turvallisuuden ohjelma omalle koululle (pptx)
eS 9.2a	eSafety Label – arviointityökalu (pptx)
eS 9.3a	Luonnos digitaalisen turvallisuuden muistilista kouluille pdf
eS 9.3b	Käyttösääntöideoita mietittäväksi pdf
eS 9.4	Olemmeko valmiita omien laitteiden (BYOT) tai henkilökohtaiseen käyttöön annettujen laitteiden (1:1) käyttöön? pptx
eS 9.4a	Oman teknologian käyttö ja usein kysytyt kysymykset – vanhemmat ja oppilaat. pdf
Tukimateriaalia	Nämä aineistot voidaan laittaa saataville kurssin verkko-oppimisalueelle.
eS 9.2b	Esittely -eSafety Label pdf
eS 9.2c	Raportti -eSafety Labelin kehittäminen pdf

Kouluttajan käsikirja ja tukimateriaalit

Kurssi:

Digitaalinen turvallisuus: TURVALLISEMPI KOULU JA LUOKKAYMPÄRISTÖ

Moduuli 10: Digitaalisen turvallisuuden toimintasuunnitelman luominen

(eS 10.0)

eS 10.0: Digitaalisen turvallisuuden toimintasuunnitelman luominen

CPDLab-kurssi	**Digitaalinen turvallisuus: Digitaalisen turvallisuuden parantaminen kouluissa**
Moduulin numero	**eS 10.0**
Moduulin nimi	**Digitaalisen turvallisuuden toimintasuunnitelman luominen**
Vaatimukset moduulin suorittamiseen	• Osallistujilla tulee olla perustaidot tieto- ja viestintätekniikan käytössä. • Osallistujien tulee olla suorittanut moduulin 9.
Kesto	3 tuntia
Kurssipaikka ja moduulin rakenne	• Tämä moduuli järjestetään lähiopetuksena. • Osallistujia kehotetaan ottamaan mukaan oma kannettava tietokoneensa, sillä moduulin aikana kokeillaan opetettavia asioita käytännössä. • Lisäksi moduuliin kuuluu tehtäviä, keskustelua, ryhmätöitä ja pohdintaa.
Tarvittavat tilat ja tilajärjestelyt	• Kouluttaja tarvitsee käyttöönsä kosketustaulun, tietokoneen ja langattoman verkon. • Jokainen osallistuja tarvitsee käyttöönsä tietokoneen, jossa on Internet-yhteys. • Tiloissa tulisi olla tarpeeksi virtapistokkeita kannettaville tietokoneille. • Lisäksi osallistujat tarvitsevat tiloja, joihin hajaantua työskentelemään 3–5 hengen pienryhmissä.
Moduulin yleiskuvaus	Kaikki osallistujat (koko kurssin suorittavat osallistujat sekä rehtorit, jotka suorittavat lyhytkurssin) perehtyvät toimintasuunnitelmaesimerkkiin. Esimerkin perusteella he saavat yleiskäsityksen asioista, joita tulisi sisällyttää digitaalisen turvallisuuden toteuttamissuunnitelmaan. **Ryhmä R – Rehtorit (ja Ryhmä O, joka on käyttänyt eSafety Label -työkalua)** Osallistujat pohtivat omien koulujensa tarpeita ja kirjaavat toimenpiteitä tärkeysjärjestykseen (jatkoa edellisestä istunnosta). Heille annetaan toteuttamissuunnitelman pohja, jota he voivat halutessaan täyttää ja muokata edelleen. Heidän toteuttamissuunnitelmansa tulisi sisältää kaikki koulun eSafety Label -toimintasuunnitelman keskeiset osa-alueet. Osallistujat esittelevät muille valmiin digitaalisen turvallisuuden toteuttamissuunnitelmansa. Kysymyksille ja keskustelulle varataan aikaa.

	Kaikki osallistujat täyttävät arviointilomakkeen ja kirjoittavat viimeisen merkinnän oppimispäiväkirjaan. Heille jaetaan todistukset.
Moduulin tavoitteet	• Laatia toteuttamissuunnitelma, jossa nimetään keskeisimmät asiat, joita koulun digitaalisen turvallisuuden kehittyminen edellyttää. • Ymmärtää, mitä toimenpiteitä koulussa tarvitaan, jotta sen digitaalisen turvallisuuden taso olisi hyvä. • Ymmärtää, että hyvä digitaalisen turvallisuuden taso vaatii jatkuvaa sitoutumista asiaan. • Kannustaa osallistujia soveltamaan digitaalisen turvallisuuden osaamistaan käytännössä. • Arvioida kurssia kokonaisuutena. • Antaa osallistujille mahdollisuus pohtia oppimistaan kurssin aikana • Saada arvokasta tietoa osallistujien kokemuksista.
Taitojen ja osaamisen karttuminen tässä moduulissa	Osallistujat oppivat • hyödyntämään uusia digitaalisia taitojaan ja digitaalisen turvallisuuden osaamista • arvioimaan digitaaliseen turvallisuuteen liittyviä kysymyksiä omassa koulussaan ja soveltamaan strategioita riskien käsittelyssä • toteuttamaan digitaalisen turvallisuuden toteuttamissuunnitelman omassa koulussaan (rehtorit) • laatimaan koko koulun digitaalisen turvallisuuden ohjelman.
Tarvittavat materiaalit ja välineet	• Pääsyoikeudet ja tuki eSafety Label -tiimiltä. • Monisteet eS 10.1 ja eS 10.2b • Kouluttajalle dataprojektori ja tietokone, jossa on Internet-yhteys. • Osallistujille kannettavat tietokoneet ja pääsy langattomaan verkkoon. • Kosketustaulu tulosten esittämiseen. Pääsy kurssin tukimateriaaleihin ja oppimispäiväkirjaan.
Vaatimukset kouluttajalle	Kouluttajan tulee ymmärtää koulumaailman strategista suunnittelua ja tietää, millaisia asioita koulun digitaalisen turvallisuuden ohjelman täytyisi sisältää. Kouluttajan tulee tutustua eSafety Label -työkaluun ja käyttää sitä ennen kurssin aloitusta. Kouluttajalla tulee olla syvällinen ja monipuolinen tietämys digitaalisesta lukutaidosta, digitaaliseen turvallisuuteen liittyvistä kysymyksistä ja digitaalisen turvallisuuden opetussuunnitelmista. Kouluttajan tulee tuntea Eu-politiikka, jonka tavoitteena on tehdä Internetistä turvallisempi lasten ja nuorten näkökulmasta, Insafen materiaalit ja palvelut sekä paikallisen Safer Internet Centren materiaalit ja kansainvälinen digitaalisen turvallisuuden opetussuunnitelma.

	Kouluttajan tulee tutustua kurssin verkkoalueeseen ja kaikkiin kurssin tukimateriaaleihin, jotka on lueteltu jokaisen moduulin lopussa. Jokainen materiaali on luetteloitu kurssin, moduulin ja tehtävän mukaan, esim. eS 1.1 "Ihmisbingo digikansalaisille" Kouluttajan tulee käyttää sosiaalista kirjanmerkkipalvelua (esim. www.delicious.com tai Diigo www.diigo.com), jonne tallennetaan digitaaliseen turvallisuuteen liittyviä linkkejä ja materiaaleja. Kouluttajan tulee myös kannustaa osallistujia luomaan oma käyttäjätili kurssilla jaettujen verkkomateriaalien hallinnoimiseksi. Kouluttajan tulee perustaa oppimisblogi ja antaa sen käyttäjätunnukset ja salasana osallistujille. Sen lisäksi kouluttajan täytyy osata käyttää ryhmätyösovelluksia, Twitteriä, blogeja jne.
Lähdeaineistot ja materiaalit kouluttajalle	**eSafety Label kouluille** www.eSafetylabel.eu/ **Insafe** www.saferInternet.org Osittain Euroopan unionin rahoittama Insafe on eurooppalainen Safer Internet Centre -verkosto, joka edistää turvallista ja vastuullista Internetin ja mobiililaitteiden käyttöä nuorten keskuudessa. Se tarjoaa laajan valikoiman materiaaleja ja tietolähteitä useilla eri kielillä. Jokaisella jäsenmaalla on oma **Safer Internet Awareness Centre.** On mahdollista hyödyntää myös muiden maiden (esimerkiksi englannin- tai ruotsinkielisiä) Safer Internet Awareness Centre-aineistoja. **Safer Internet Day** (SID) www.saferInternetday.org Helmikuun toisena tiistaina vietetään kouluissa vuosittain kansainvälistä Internet-turvallisuuden teemapäivää (Safer Internet Day). EU:n hanke tarjoaa materiaaleja, oppituntisuunnitelmia ja teemapaketteja opettajille ja kouluille. **Euroopan komissio** "Eurooppalainen strategia Internetin parantamiseksi lasten näkökulmasta", saatavana useilla eri kielillä: http://ec.europa.eu/information_society/activities/sip/policy/index_en.htm **Teach today** www.teachtoday.eu/ Teachtoday-sivusto tarjoaa opettajille, rehtoreille ja muille koulun työntekijöille tietoa ja neuvoja uuden tekniikan myönteiseen, vastuulliseen ja turvalliseen hyödyntämiseen. Sivustolla olevien tapausesimerkkien avulla kouluttajat voivat herättää keskustelua osallistujien kohtaamista todellisista ongelmista kouluissa. www.teachtoday.eu/en/Case-studies.aspx **Byron Review –raportti** www.dcsf.gov.uk/byronreview ”Safer Children in a Digital World” (Digitaalinen maailma turvallisemmaksi lapsille)

Arviointivaihtoehdot	• Osallistujat kirjoittavat viimeisen merkinnän oppimisblogiin. • Osallistujat kertovat kurssin kohokohdista ja tulevaisuuden suunnitelmistaan.
Moduulin jälkeiset jatkotoimenpiteet	• Osallistujien kouluissa toteutetaan koko koulun digitaalisen turvallisuuden toteuttamissuunnitelma. • Koulu valmistautuu seuraavaan arviointiin (kahden vuoden päästä) eSafety Label -työkalun avulla.
Vaihtoehtoiset tavat toteuttaa moduuli	Tämä moduuli voidaan järjestää seuraaville kohderyhmille: • **Ryhmä O:** Opettajat, jotka suorittavat kaikki 10 moduulia TAI • **Ryhmä R: Rehtorit** ja TVT-koordinaattorin tehtäviä hoitavat opettajat Aktiviteetit **Ryhmälle O** ja **Ryhmälle R** on määritelty tarkemmin jokaisen tehtävän kohdalla.
Toteuttamisvaihtoehdot kansallisella/paikallisella tasolla	Tämä moduuli voidaan toteuttaa kansallisella/paikallisella tasolla. **Tiedoksi paikallisille kouluttajille** Saatavilla on monia muitakin ilmaisia työkaluja digitaalisen turvallisuuden itsearviointia varten. Paikallisille osallistujille voi näyttää heidän omassa koulutusjärjestelmässään käytetyn työkalun, kuten 360safe tai The Online Compass (tarkoitettu erityisesti nuorisoryhmille). Osallistujat voivat halutessaan valita työkalun, joka tuntuu heille sopivimmalta, ja syöttää tietoja siihen. Katso myös: eS 10.2d Itsearviointityökalu kouluille digitaalisen turvallisuuden 360 asteen arviointiin
Tehtävä 10.1:	**Esimerkki toimintasuunnitelmasta**
Kesto	40 min
Tavoitteet	• Ymmärtää, millaisia asioita koulun eSafety Label -toimintasuunnitelman täytyy sisältää ja mitä pidetään hyvinä käytäntöinä. • Lukea ja tulkita eSafety label -sovelluksen antamaa toimintasuunnitelmaa • Keskustella siitä, kuinka asettaa koulun digitaalisen turvallisuuden ohjelman parantamiseksi tarvittavat toimenpiteet tärkeysjärjestykseen.
Kuvaus	**Tehtävä 1** Jaa osallistujille materiaali eS 10.1 Esimerkki eSafety Label -toimintasuunnitelmasta (fiktiivinen esimerkki Stamaryn koululta) ja aloita keskustelu siitä, kuinka näitä tietoja voitaisiin hyödyntää. Mitkä ovat Stamaryn koulun keskeiset ongelmat?

	Kouluttaja jakaa ryhmän kolmeen pienempään ryhmään, joista jokainen tarkastelee itseään kiinnostavaa osa-aluetta: koulun tieto- ja viestintäteknin-en infrastruktuuri, toimintaohjeet tai opetussuunnitelma. Ryhmät keskus-televat Stamaryn toimintasuunnitelmasta ja jokainen ryhmä pyrkii asetta-maan keskeiset muutoskohteet tärkeysjärjestykseen. Mitkä digitaalisen turvallisuuden osa-alueet – henkilökohtainen turvallisuus ja hyvinvointi, digitaalinen lukutaito ja digikansalaisuus – ovat tarpeellisim-pia sisällyttää koko opetussuunnitelmaan? Mitä sisäistä täydennyskoulutus-ta Stamaryn koulun henkilökunta tarvitsee? **Palaute** Jokainen ryhmä kertoo tuloksistaan ja kouluttaja kokoaa kosketustaululle listan muutoskohteista. Kuinka paljon muutoksia koulu voi aikataulun puo-lesta suunnitella tai toteuttaa lukukauden/kouluvuoden aikana? Mikä on toteutettavissa? Mikä vaatii nopeita toimia? **Tehtävä 2** Kouluttaja jakaa osallistujille materiaalin eS 10.2b Toteuttamissuunnitelman pohja (HUOM.: Pohjaa käytetään tehtävässä 10.2) Ryhmä keskustelee kou-luttajan johdolla pohjan suunnitelmamallista. Kuinka Stamaryn koulun tulisi asettaa tärkeysjärjestykseen ja aikatauluttaa digitaaliseen turvallisuuteen liittyvät toimenpiteet? Kuinka tässä voitaisiin käyttää esimerkkisuunnitel-maa? Kuinka sen avulla voidaan asettaa Stamaryn koulun digitaalisen tur-vallisuuden järjestelyt tärkeysjärjestykseen?
Tehtävä 10.2	**eSafety Label -toimintasuunnitelman käyttäminen koulun digitaalisen turvallisuuden ohjelman kehittämisessä**
Kesto	1 h
Tavoitteet	• Suunnitella koulun digitaalisen turvallisuuden ohjelmaa. • Miettiä tulevaisuuden toimenpiteitä omassa koulussa. • Jokainen osallistuja valmistelee oman toimintasuunnitelmansa kou-lunsa digitaalisen turvallisuuden parantamiseksi.
Kuvaus	**Tehtävä 1** Osallistujat avaavat koulunsa eSafety Label -profiilin www.esafetylabel.eu ja lounaan aikana valmistuneen eSafety Label -toimintasuunnitelman. Osallistujat lukevat ja arvioivat eSafety Label -toimintasuunnitelmansa. He perehtyvät verkossa joihinkin tietosivuihin, tietoihin ja ehdotettuihin työka-luihin. Osallistujat pohtivat, mitä asioita heidän kouluissaan on jo toteutet-tu ja tuovat esille, millä digitaalisen turvallisuuden alueilla on vielä puutteita. Tämä tehtävä tehdään yksin. Kouluttaja voi ehdottaa lisätietolähteitä – Insafe, paikalliset Safer Internet Awareness Centre -sivustot, kansainväliset opetussuunnitelmat.

	Tehtävä 2 Osallistujat käyttävät tyhjää pohjaa eS 10.2b Toteuttamissuunnitelman pohja, johon jokainen täyttää oman digitaalisen turvallisuuden toiminta-suunnitelmansa. Tyhjän toteuttamissuunnitelmapohjan avulla osallistujat päättävät osa-alueet, joihin keskitytään, ja vastaavat seuraaviin kysymyksiin: • Mitkä ovat omassa koulussani keskeisiä opetussuunnitelmaan/toimintaohjeisiin/tieto- ja viestintätekniseen infrastruktuuriin liittyviä kysymyksiä? • Mitkä digitaalisen turvallisuuden osa-alueet – henkilökohtainen turvallisuus ja hyvinvointi, digitaalinen lukutaito ja digikansalaisuus – tarvitsevat eniten suunnittelua? • Minkälaista koulun sisäistä täydennyskoulutusta opettajat tarvitsevat? **Tehtävä 3** Osallistujat keskustelevat pareittain, vertailevat koulujensa tilannetta ja keräävät yhdessä ideoita siihen, miten edetä koulunsa digitaalisen turvallisuuden suunnitelman kanssa. Kouluttaja tuo esiin tarpeen digitaalisen turvallisuuden neuvostolle, jossa oppilaat ovat mukana toimintaohjeiden valmistelussa muiden tahojen ohella. Jokainen osallistuja valmistelee oman suunnitelmansa koulunsa digitaalisen turvallisuuden parantamiseksi.
Kahvitauko	**15 min**
Tehtävä 10.3:	**Keskustelua – seuraavat vaiheet?**
Kesto	15 min
Tavoitteet	• Esitellä osallistujien toteuttamissuunnitelmat. • Antaa toisille tukea. • Päättää seuraavista toimenpiteistä ja kertoa ne ryhmälle.
Kuvaus	• Kouluttaja etsii humoristisen muutos- tai suunnitteluprosessia kuvaavan videon, esim. norjalainen Kirja (hakusanalla Medieval helpdesk YouTubessa). • Kouluttaja johdattaa osallistujat keskusteluun seuraavista vaiheista sekä antaa osallistujien kertoa toisilleen toimintasuunnitelmistaan ja jakaa niitä.
10. 4	**Johtopäätökset ja arviointi**
Kesto	30 min
Tavoitteet	• Arvioida omaa oppimista kurssin aikana. • Päättää kurssi jakamalla kurssin kohokohtia sekä parhaita aineistoja

	ja työkaluja. • Antaa mahdollisuus tarkastella omaa oppimispäiväkirjaa. • Kurssiarvioinnin tekeminen. • Kurssitodistusten jakaminen.
Kuvaus	Lopullinen itsearviointi oppimispäiväkirjaan • Mitä vien mukanani takaisin omalle koululleni? • Mitä olen oppinut kurssin aikana ja mitä kerron kollegoilleni? • Osallistujat jakavat hauskan linkin (esim. hauska video) jäähyväisiksi ryhmälle. • Osallistujat täyttävät kurssin arviointilomakkeen. eS 10.4a Kurssin arviointi URL **Keskustelurinki** Jokainen kertoo muille yhden kurssin kohokohdan ja toimenpiteen, jonka he toteuttavat kotiin/koululle palattuaan. Ryhmä keskustelee, kuinka he pitävät tulevaisuudessa yhteyttä ja heille kerrotaan webinaarin (jos sellainen järjestetään) yksityiskohdista. Kouluttaja jakaa osallistujille kurssitodistukset.
Tehtävä 10.6	**Kurssin päätös**
Kesto	10 min
Tavoitteet	Päätössanat ryhmälle
Kuvaus	Kouluttaja jakaa ryhmälle 1–2 hauskaa linkkiä ja pitää lyhyen rohkaisevan jäähyväispuheen.

Moduuli 10: KURSSIN TUKIMATERIAALIT

Kurssi/Moduuli/Tehtävä	Kurssin tukimateriaalit
eS 10.1	Esimerkki eSafety Label -toimintasuunnitelmasta (pdf)
eS 10.2b	Toteuttamissuunnitelman pohja (doc)
Tukimateriaalia	Nämä aineistot voidaan laittaa saataville kurssin verkkoalueelle.
eS 10x	Yhteenveto tutkimustuloksista (pdf)

eS 10.2c	Hyvien ja riittämättömien käytäntöjen tunnusmerkkejä (pdf)
eS 10.2d	Itsearviointityökalu kouluille digitaalisen turvallisuuden 360 asteen arviointiin (pdf)

TIETOJA TÄSTÄ ASIAKIRJASTA

Tämä asiakirja on luotu osana Euroopan komission rahoittamaa CPDLab-projektia.

Creative Commons

CPDLab-kumppaneita

European Schoolnet

Indire
Istituto Nazionale di Documentazione, Innovazione e Ricerca Educativa

direção-geral da educação

THE NORWEGIAN CENTRE FOR ICT IN EDUCATION

FINNISH NATIONAL BOARD OF EDUCATION

UNIVERSITY of OULU
OULUN YLIOPISTO

Yhteystiedot

Verkkosivusto: http://cpdlab.eun.org

Sähköposti: info@eun.org

Vastuuvapauslauseke

Tässä asiakirjassa esitettyä sisältöä tukee Euroopan komission elinikäisen oppimisen ohjelman alainen projekti CPD*Lab*: Continuing Professional Development Lab (avustussopimus 2011-3641/001-001). Tämän asiakirjan sisällöstä vastaavat ainoastaan projektikumppanit. Se ei edusta Euroopan komission mielipiteitä eikä komissio ole vastuussa siihen sisältyvien tietojen mahdollisesta käytöstä.

Lifelong Learning Programme