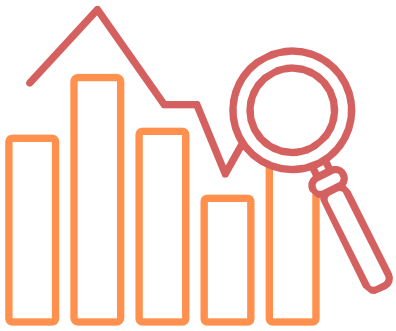
Co-funded by
the European Union

Okvir kompetenc digitalne suverenosti



Co-funded by
the European Union

Projekt je podprla Evropska komisija v okviru programa Erasmus+. Ta publikacija odraža le stališča avtorja in Komisija ne more biti odgovorna za kakršno koli uporabo informacij, ki jih vsebuje.

Preberite več o

LINKS

Kazalo vsebine

Uvodni del

Cilj projekta LINKS je podpreti evropske mladinske delavce pri doseganju njihove lastne podatkovne suverenosti in izboljšanju njihovih veščin digitalne varnosti z novo, inovativno obliko vsebine usposabljanja v podporo razvoju digitalnih kompetenc.

V začetnih fazah načrtovanja tega projekta in aplikacije je analiza potreb potrdila dejstvo, da v Evropi trenutno ni enotnega okvira digitalne suverenosti in varnosti.

DigComp (okvir digitalnih kompetenc) se sklicuje na številne splošne in splošne temeljne spretnosti in kompetence, povezane z digitalno varnostjo na splošno, in ta rezultat se bo skliceval na ta obstoječi okvir kompetenc, vendar je posebej usmerjen v proaktivno ozaveščanje mladinskih delavcev po Evropi o trenutno obstoječih grožnjah digitalni varnosti.

Okvir kompetenc za digitalno suverenost opredeljuje ključne sestavine kompetenc, ki jih mladinski delavci potrebujejo za učinkovito vključevanje digitalne suverenosti in varnostnih protokolov v svoj lokalni kontekst, ter zagotavlja in potrjuje referenčni okvir EU za razvoj in vrednotenje kompetenc na področju digitalne varnosti. Kompetence digitalne varnosti so močno povezane s splošnimi digitalnimi kompetencami in se ne štejejo za samostojne kompetence.

Okvir je namenjen mladinskim delavcem, vendar je pomemben in zanimiv tudi za učitelje in vodje usposabljanj na področju IKT pred začetkom dela in med delom ter vzgojitelje, pa tudi za oblikovalce politik na področju izobraževanja in vseživljenjskega učenja v zvezi s tehnološkim izpopolnjevanjem in krepitvijo zmogljivosti posameznikov.

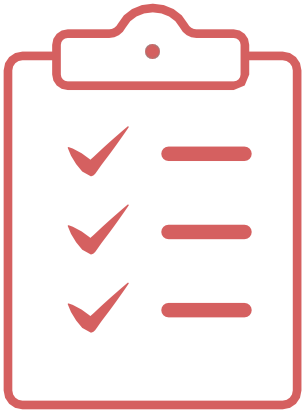
Pričakujemo, da bodo nevladne organizacije za digitalno usposabljanje in organizacije za usposabljanje po vsej Evropi sprejele ta okvir kot del svojih izobraževalnih dejavnosti ocenjevanja in poučevanja, kar bo dolgoročno povečalo ozaveščenost in spodbudilo vključitev okvira v lokalne, regionalne in nacionalne digitalne izobraževalne organe v evropskih državah.

Ugotovitve projektne ankete in fokusnih skupin

Okvir kompetenc digitalne suverenosti temelji na metodologiji in ugotovitvah projektne raziskave in fokusnih skupin. Prav tako se želi uskladiti z okvirom DigComp, ki podpira dolgoročno izkoriščanje in trajnost kot dodatni okvir kompetenc, specifičen za ciljno skupino.

Projektna raziskava je pripomogla k spoznavanju uporabe tehnologije in varstva podatkov v digitalnih delovnih praksah mladinskih delavcev. Mladinski delavci potrebujejo večjo ozaveščenost v kombinaciji z dobrim upravljanjem digitalnih identitet, to lahko pomaga omejiti dogodke, ki jih povzroči "nepozornost" uporabnika ali same organizacije. Pisali so o potrebi po vzpostavitvi in sporočanju varnostnih politik za delo na daljavo, o urejanju uporabe osebnih naprav, varovanju komunikacijskih kanalov in kanalov za sodelovanje ter zagotavljanju budne informacijske podpore. Priporočili so, naj bodo tečaji na voljo večjemu številu zaposlenih in m l a d i h , naj se uporabljajo ustreznejši primeri v zvezi s konkretnimi nalogami, izboljša mreženje ter izmenjava dobrih in slabih izkušenj na spletu. Pomembno je, da se stalno posodablja, zlasti z novimi dokumenti EU.

Večina mladinskih delavcev ni bila deležna usmerjenega usposabljanja, odločitve o spletni varnosti sprejemajo na podlagi lastnega znanja. Zapisali so, da je treba te vidike poglobiti za varnost organizacij in zasebnih uporabnikov ter organizirati posebno usposabljanje za pooblaščence za varstvo podatkov.



Potreba po okviru kompetenc digitalne suverenosti

Vedno večja je zaskrbljenost, da državljani, podjetja in države članice Evropske unije postopoma izgubljajo nadzor nad svojimi podatki, inovacijsko zmogljivostjo ter zmožnostjo oblikovanja in uveljavljanja zakonodaje v digitalnem okolju. Glede na to se krepi podpora novemu političnemu pristopu, ki naj bi povečal strateško avtonomijo Evrope na digitalnem področju.

Tehnološka podjetja zbirajo ogromne količine osebnih podatkov, zato se je v EU povečala skrb, kako lahko evropski državljani ponovno pridobijo nadzor nad svojimi digitalnimi podatki v spletnem okolju, v katerem zdaj prevladujejo predvsem tehnološka podjetja zunaj EU.

Ker se mladinsko delo vse bolj prilagaja digitalnemu svetu, opažamo, da tudi mladinski delavci sprejemajo nove pristope. Čeprav je digitalni svet nov in vznemirljiv ter ponuja nešteto priložnosti, ga je treba v okviru mladinskega dela bolje razumeti. Pri kompetencah digitalne suverenosti je potrebnih več ukrepov, da bi popisali obstoječe prakse, platforme, orodja in učne okvire digitalnega mladinskega dela.

Digitalna suverenost je nov pojem v digitalni dobi, ki se običajno razume kot "sposobnost posameznikov, da si lastijo svoje zasebne podatke in nadzorujejo njihovo uporabo".

Pandemija COVID-19 je močno vplivala na vsakdanje življenje večine posameznikov. Kot odgovor na to je bila prilagojena tehnologija, ki je poskušala ublažiti te učinke in posameznikom ponudila digitalne alternative za številne vsakodnevne dejavnosti, ki jih ni več mogoče opravljati normalno. Navidezno druženje in spletni dogodki so postali običajni in so v veliki meri pripomogli k temu, da ljudje med zaprtjem niso popolnoma izolirani.

Spletno izobraževanje je marsikje postalo tudi nova stalnica, saj šole in univerze uporabljajo spletne razrede, da bi zagotovile nemoteno izobraževanje študentov. Poleg tega se je zaradi prožnejših urnikov posameznikov ali več prostega časa med zaprtimi urami močno povečalo število ljudi, ki uporabljajo osebna orodja za učenje in razvoj, kot so aplikacije za učenje jezikov. Tudi zdravstvo se je usmerilo k digitalnim rešitvam in omogočanje spletne dostopnosti tako duševnega kot fizičnega zdravstvenega varstva je postalo bolj pogosto in je dokaj uspešno pomagalo ublažiti negativne učinke zmanjšanega dostopa do zdravstvenega varstva.

Obstoječi ustrezni okviri

Razviti so bili različni okviri digitalnih pedagoških kompetenc, ki podpirajo učinkovit in smiseln profesionalni razvoj digitalnih pedagoških kompetenc strokovnih učiteljev, ki temelji na merilih.

Evropski okviri, objavljeni v zadnjih letih, opisujejo, kako naj bi izgledala digitalno kompetentna izobraževalna organizacija DigCompOrg in digitalno kompetentno pedagoško osebje DigCompEdu, ter spodbujajo organizacije, da zagotovijo kompetence svojega osebja in razvijejo nacionalne rešitve za zagotavljanje digitalnih kompetenc.

DigCompEdu je okvir digitalnih kompetenc, katerega ciljna skupina so predvsem univerzitetni profesorji in zaposleni.
Okvir DigComp opredeljuje ključne sestavine digitalne usposobljenosti n a petih področjih:

1. Informacijska in podatkovna pismenost: Informacijska pismenost: izražanje informacijskih potreb, iskanje in pridobivanje digitalnih podatkov, informacij in vsebin. presojati ustreznost vira in njegove vsebine. shranjevanje, upravljanje in urejanje digitalnih podatkov, informacij in vsebin.
2. Komunikacija in sodelovanje: Sodelovanje: interakcija, komuniciranje in sodelovanje z digitalnimi tehnologijami ob upoštevanju kulturne in generacijske raznolikosti. Sodelovanje v družbi prek javnih in zasebnih digitalnih storitev ter participativnega državljanstva. Upravljati svojo digitalno prisotnost, identiteto in ugled.
3. Ustvarjanje digitalnih vsebin: Ustvarjanje in urejanje digitalnih vsebin Izboljšanje in vključevanje informacij in vsebin v obstoječe znanje ob razumevanju uporabe avtorskih pravic in licenc. znati dati razumljiva navodila za računalniški sistem.
4. Varnost: Zaščita naprav, vsebine, osebnih podatkov in zasebnosti v digitalnih okoljih. Varovanje fizičnega in psihičnega zdravja ter zavedanje digitalnih tehnologij za družbeno blaginjo in socialno vključenost. Zavedati se vpliva digitalnih tehnologij in njihove uporabe na okolje.
5. Reševanje problemov: Reševanje problemov: prepoznavanje potreb in problemov ter reševanje konceptualnih problemov in problemskih situacij v digitalnih okoljih. Uporaba digitalnih orodij za inoviranje procesov in izdelkov. Biti na tekočem z digitalnim razvojem.

Obstaja konceptualni referenčni model DigComp, v katerem je 21 kompetenc, ki se nanašajo na ta področja. Dodatne dimenzije opisujejo ravni usposobljenosti, znanja, spretnosti in odnosa ter primere uporabe.

Okvir kompetenc digitalne suverenosti za mladinske delavce

Na podlagi raziskave in analize obstoječih okvirov so se partnerji tega projekta odločili, da se bodo osredotočili na štiri varnostne teme DigiComp in dodali tudi kompetence, ki so posebej potrebne za mladinske delavce. Tukaj so kompetence iz okvira DigiComp:

4.1 Zaščita naprav

Zaščita naprav in digitalne vsebine ter razumevanje tveganj in groženj v digitalnih okoljih. poznati varnostne in varovalne ukrepe ter ustrezno upoštevati zanesljivost in zasebnost.

4.2 Zaščita osebnih podatkov in zasebnosti

Zaščita osebnih podatkov in zasebnosti v digitalnih okoljih. Razumeti, kako uporabljati in deliti osebne podatke ter hkrati zaščititi sebe in druge pred škodo. Razumeti, da digitalne storitve uporabljajo "pravilnik o zasebnosti" za obveščanje o tem, kako se uporabljajo osebni podatki.

4.3 Varovanje zdravja in dobrega počutja

Da bi se lahko pri uporabi digitalnih tehnologij izognili zdravstvenim tveganjem ter grožnjam za fizično in psihično dobro počutje. znati zaščititi sebe in druge pred morebitnimi nevarnostmi v digitalnih okoljih (npr. kibernetskim ustrahovanjem). Zavedati se digitalnih tehnologij za socialno blaginjo in socialno vključenost.

4.4 Varovanje okolja

Zavedati se vpliva digitalnih tehnologij in njihove uporabe na okolje.
https://joint-research-centre.ec.europa.eu/digcomp/digital-competence-framework_en#ref-4-safety _

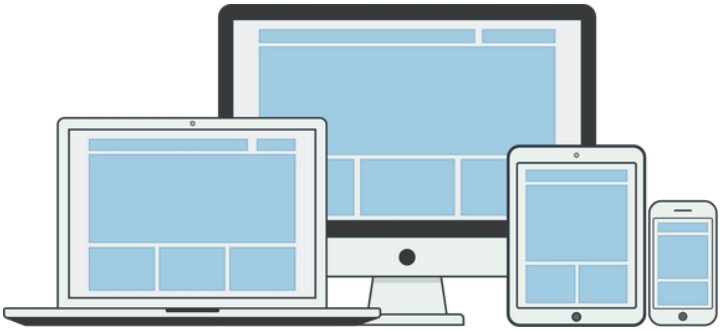
Pri opredeljevanju osnovnih digitalnih kompetenc za mladinske delavce je koristno razmišljati tako o univerzalnih (DigComp kompetence za državljane) kot o specifičnih (vsakodnevne dejavnosti pri mladinskem delu) značilnostih praktičnega učenja, ki iz tega izhajajo.

Pristojnosti za varstvo osebnih podatkov in zasebnosti

* tehnično znanje digitalnih tehnologij,
* sposobnost smiselne uporabe digitalnih tehnologij pri delu, študiju in drugih vsakodnevnih dejavnostih,
* sposobnost kritičnega vrednotenja digitalnih tehnologij;
* poznati osnovna pravila o spletni varnosti;
* da bi razumeli, kako deluje splet;
* razumeti, kaj je e-trženje in kako deluje;
* razumevanje zasebnosti in poznavanje pravic intelektualne lastnine;
* vedeti, kako izvajati varnostne ukrepe;
* razvijanje samoučinkovitosti pri uporabi digitalnih tehnologij.

Pristojnosti za zaščitne naprave

Zaščita računalnika in pametnega telefona z močno in posodobljeno varnostno programsko opremo. Če je računalnik ali telefon okužen z zlonamerno programsko opremo, vam druga zaščitna sredstva ne pomagajo kaj dosti, saj imajo kriminalci morda že ključ do vseh spletnih dejanj. Pomembno je tudi, da se prepričate, da so nameščene vse posodobitve operacijskega sistema. Mladinski delavci morajo poskrbeti za vse svoje naprave. Te morajo biti posodobljene in opremljene z učinkovito protivirusno programsko opremo. Različni proizvajalci izdajajo posodobitve, ki ne le izboljšujejo funkcije, temveč tudi odpravljajo morebitne varnostne pomanjkljivosti, ki bi lahko postavile naprave.
ogroženi. Splošno varnostno pravilo je, da za dejavnosti, ki zahtevajo prijavo v katero koli od storitev, ki jih uporabljate, ne uporabljate nobenega drugega računalnika ali naprave.



Naučite se prepoznati neželeno pošto in prevare

Čeprav je nekatere poskuse goljufanja v e-pošti, družabnih omrežjih ali spletnih mestih enostavno prepoznati, so lahko drugi videti zelo legitimni. Edini način, da ne boste nikoli nasedli goljufiji, je, da nikoli ne kliknete na poslano povezavo. Če e-poštno sporočilo navaja, da je od banke, ima vse prave logotipe in pozna ime, je morda od prave banke ali pa tudi ne. Namesto uporabe posredovane povezave lahko pri preprečevanju prevare pomagata iskanje spletnega mesta in uporaba iskalnika. Tako bo uporabnik vedel, ali je pristal na legitimnem spletnem mestu in ne na izmišljenem lažnem spletnem mestu.

uporaba uglednih spletnih strani pri nakupih.

Če uporabnik ne pozna ugleda podjetja, pri katerem želi opraviti nakup, je pomembno, da pred tem preuči spletno mesto. Vprašajte: "Kako jih ocenjujejo drugi uporabniki?" "Ali uporabljajo varno, šifrirano povezavo za osebne in finančne podatke?"

Ostanite pozorni

previdnost pri uporabi javnih omrežij WiFi in dvakratno premislek, preden se pridružite nezavarovanemu omrežju. Obstajajo orodja, ki lahko uporabniku pomagajo zagotoviti več zasebnosti in ga med brskanjem zaščitijo pred drugimi uporabniki in samimi spletnimi mesti v javnih omrežjih WiFi.

Varnost na spletu

Spletni svet je postal tako hitro spreminjajoče se okolje, da so lahko današnji nasveti že jutri zastareli. Mladinski delavci se morajo zavedati, da je treba vsebine, ki jih uživajo (in včasih jih je res veliko), filtrirati. Pomembno je, da ste nekoliko sumničavi. Na internetu je relativno enostavno ponarediti stvari. Zelo lahko je na internetu objaviti nekaj, kar ni povsem resnično ali pa je le skupek laži. Še posebej moramo paziti, da ne verjamemo vsemu, kar vidimo in preberemo na internetu. Kot dober nasvet velja, da se moramo poglobiti in razločiti, kaj je res in kaj ne, če imamo o čemer koli najmanjši dvom. Poskusite biti kritični do stvari na spletu in tako zmanjšajte tveganje, povezano z vsemi spletnimi dejavnostmi.

Deljenje informacij v družabnem omrežju

"Izmenjava informacij opisuje izmenjavo podatkov med različnimi organizacijami, ljudmi in tehnologijami" (Techopedia). Obstaja več vrst izmenjave informacij:

- informacije, ki jih posamezniki delijo (na primer videoposnetek, ki ga delijo na Facebooku ali YouTubu);
- Informacije, ki jih delijo organizacije (na primer vir RSS spletnega vremenskega poročila);
- informacije, ki si jih izmenjujeta vdelana/programska oprema (na primer naslovi IP razpoložljivih omrežnih vozlišč ali razpoložljivost prostora na disku).

Vsa družbena omrežja (ali večina njih) uporabnikom omogočajo, da ustvarijo poljubno podrobne profile. V nekaterih primerih ta postopek uporabnikom pomaga najti druge uporabnike s skupnimi interesi itd. V družabnih omrežjih, kot je Facebook, je mogoče spremeniti nastavitve zasebnosti in tako nadzorovati, katere informacije so javne in katere so namenjene samo "prijateljem". Vendar je pomembno vedeti, da ima te informacije ne glede na nastavitve zasebnosti tudi samo družbeno omrežje.

Običajno ljudje delijo starost, spol, družino, druge interese, izobrazbo in podrobnosti v zvezi z lastno zaposlitvijo. Objavljanje slik ali "statusov" je hiter način za prikazovanje občutkov, situacij in izmenjavo informacij. Večina družabnih omrežij je zasnovana tako, da to doseže na najhitrejši možni način. Zavedati se, katere so stvari, ki jih uporabnik deli, je resnično pomembno. Z deljenjem so izpostavljene informacije, ki oglaševalcem omogočajo sledenje preferencam in okusom potencialnih potrošnikov.

GDPR

GDPR se je za vse članice EU in EGP začela uporabljati 25. maja 2018. Nadomestila je današnjo zakonodajo o zasebnosti v državah članicah, za katere trenutno velja Direktiva EU 95/46. GDPR je na nekaterih področjih podrobnejša in natančnejša ter upošteva izzive v hitro razvijajočem se digitalnem svetu, zaradi česar nastajajo tveganja za zasebnost posameznikov, na katere se nanašajo osebni podatki.

Reference

Varstvo podatkov in spletna zasebnost https://europa.eu/youreurope/citizens/consumers/internet-telecoms/dataprotection-online-privacy/i ndex_en.htm

Techopedia https://www.techopedia.com/definition/24839/information-souporaba

Navodila po korakih za nastavitev računalnika in ustvarjanje uporabnika https://www.wikihow.com/Use-a-Computer

Pravice do zasebnosti https://www.privacyrights.org/consumer-guides/social-networking-privacy-kako biti-varen-varen-in-socialen