

## Priporočila za šole in učitelje pri izobraževanju na daljavo – varnostni vidik

September 2020

V času letošnje karantene so se vzpostavile različne prakse pri izobraževanju na daljavo. Pouk na daljavo bo zelo verjetno do neke mere prisoten tudi v šolskem letu 2020/21. Da se boste lahko lažje pripravili nanj in lažje skrbeli za varnost učencev in dijakov, smo na Točki osveščanja o varni rabi interneta Safe.si v sodelovanju z ARNES in Logout pripravili nekaj priporočil za varen pouk na daljavo. V priporočilih smo zajeli najbolj ključna področja, svetujemo pa vam tudi, da obiščete spletna mesta, navedena na koncu priporočil, kjer boste dobili še več nasvetov, informacij in nasvetov za varno rabo interneta.

Predvsem varovanje zasebnosti učencev, učiteljev in staršev je bilo eden izmed najbolj izpostavljenih izzivov te pomladi. Ker zaradi nepričakovanih razmer nihče ni mogel biti pripravljen na prehod na izobraževanje na daljavo, je bila večina šol in učiteljev prisiljena v bolj ali manj improviziran pristop. Pri pripravi poučevanja na daljavo so mnogi izobraževalci uporabljali različne brezplačne rešitve, ki so v lasti organizacij, ki nimajo sedeža v EU. Številne izmed njih, v zameno za ponujeno »brezplačno« storitev, zahtevajo dostop do različnih uporabniških podatkov (osebnih podatkov, vedenjskih vzorcev, lokacijskih podatkov ...), s čimer pa je lahko ogrožena zasebnost in s tem tudi varnost uporabnikov.

Poleg tega pa so bili nekateri učenci po nepotrebem izpostavljeni različnim tveganjem zaradi šolskih nalog, kot so bile na primer različne video naloge tipa »Posnemi se pri tem, ko pečeš piškote, delaš počepe ...« ali »Posnemi se pri dnevni rutini«. Učitelji so lahko s takimi nalogami ogrozili zasebnost učencev, njihovih družin ter doma in jih izpostavili možnostim zlorab teh posnetkov.

### Splošna priporočila

Pri šolanju na daljavo je treba zagotavljati **varnost in varovanje zasebnosti za učence, njihove starše, učitelje in vse druge v gospodinjstvih**, od koder poteka šolanje na daljavo.

**Šola naj oblikuje šolska pravila za uporabo orodij za poučevanje na daljavo.** Pri izbiri orodij naj se šola ravnava po priporočilih Ministrstva za izobraževanje, znanost in šport.

**Uporaba nabora orodij za poučevanje na daljavo naj bo usklajena na nivoju šole.** Pri tem je treba poskrbeti, da so vsi učitelji, učenci in starši seznanjeni s tem, katera orodja se uporabljajo in kakšna so pravila uporabe teh orodij za šolske namene. Pri orodjih je treba preveriti pogoje uporabe storitve, predvsem tisti del, ki se nanaša na obdelavo in deljenje uporabniških podatkov in poskrbeti za nastavitve zasebnosti oziroma preveriti, kakšne so privzete nastavitve. V splošnem je tudi priporočljivo, da se uporabijo storitve, ki tečejo na strežnikih v EU oziroma v državah, ki imajo podobno zakonodajo o varovanju zasebnosti kot EU.

**Šola naj za učence in starše pripravi natančna navodila za uporabo orodij in učence nauči ta orodja uporabljati na varen način, vključno z bontonom.** Ta navodila naj vsebujejo tudi iztočnice za pogovor

z učenci o varni in odgovorni rabi posameznega orodja. Prav tako lahko vključujejo pravila lepega vedenja, bontona pri učenju prek interneta (kdaj lahko kontaktiramo z učiteljem in ostale prek spleta, kako vljudno komuniciramo prek spleta, ali je treba potrditi prejem določenega sporočila, elektronske pošte s kratkim odgovorom ipd. ). **Na nivoju šole je treba uskladiti politiko deljenja osebnih podatkov.** Pomembno je, da se te politike in pravil varovanja zasebnosti striktno držijo vsi zaposleni na šoli.

**Za uporabo različnih aplikacij in storitev s strani učencev in dijakov,** kjer se morajo za uporabo registrirati ali ustvariti lastne račune, **je treba pridobiti soglasje staršev,** če so mlajši od 16 let. Če starši soglasja ne dajo, potem otrok teh storitev ne sme uporabljati.

**Za varovanje zasebnosti učencev in učiteljev je priporočljiva uporaba AAI prijave,** kjer je to seveda možno, saj pri tem osebni podatki uporabnikov ostajajo v upravljanju šole, k ponudniku pa se prenesejo le podatki, potrebni za delovanje storitve. Zelo pomembna so tudi **močna gesla,** ki si morajo biti med seboj različna za vsako storitev.

**Pri videokonferenčni komunikaciji je potrebno vse vpletene (učitelje, učence in starše) opozoriti na ozadje, ki je vidno na posnetku in lahko razkriva tudi kaj, česar nekdo morda ne želi deliti z drugimi** ali pa kaj, kar bi ga lahko izpostavilo vrstniškemu nadlegovanju ali kaki drugi zlorabi. Uporabljajo naj nevtralna ozadja (npr. belo steno), ozadje zamegljijo ali uporabijo virtualno ozadje. Treba je tudi spoštovati zasebnosti drugih članov družine, ki bi se morebiti znašli v ozadju med video konferenco.

Isto velja tudi za video posnetke, ki jih za pri šolanju na daljavo izdelujejo učenci. Pred tem je učence in starše treba opozoriti, da **naj ti posnetki ne prikazujejo ničesar, za kar ne želijo, da je vidno drugim.** Prav tako ni dopustno od učencev zahtevati, da morajo v posnetke vključevati druge člane družine. Lahko jih prosijo za sodelovanje, vendar naj jih nikoli ne snemajo brez njihove privolitve. Spregovorite z učenci o pravici do lastne podobe, ki jo ima vsak človek, in o nujnosti pridobitve dovoljenja, preden nekoga slikamo ali snemamo in tudi dovoljenja za nadaljnjo uporabo, objavo teh posnetkov.

Pri tovrstnih nalogah in delu na daljavo **izkoristite priložnost za pogovor z učenci o varovanju zasebnosti, o tem, kaj lahko razkrivamo prek spleta in kaj ne.** Pri izvajanju različnih nalog za pouk, ki vključujejo snemanje, vedno znova opozarjajte na razkrivanje zasebnosti. Snemanje doma lahko razkrije zasebnost otroka, družine in doma. Predmeti v ozadju lahko veliko povedo in podajo informacije, ki lahko razkrijejo lokacijo doma, navade ali drugo, kar lahko nekdo uporabi proti družini ali proti otroku. Kot primer: plišasti medvedek na polici lahko sproži norčevanje vrstnikov iz najstnika, dragocenosti lahko privabijo nepridiprave ipd.

**Pomembno je, da ima šola s pravilniki urejeno, kako učitelji obravnavajo in shranjujejo posnetke, ki jim jih posredujejo učenci.** Učitelji naj prejetih posnetkov ne shranjujejo na lastnih zasebnih računalnikih, temveč naj zato uporabljajo šolske računalnike (npr. prenosnike v lasti šole, s katerimi delajo doma). Če to ni možno, pa mora šola imeti uporabo zasebnih računalnikov in shranjevanje posnetkov učencev urejeno z ustreznim internim pravilnikom.

## Elektronska pošta in sistemi za posredovanje večjih datotek

Pri uporabi elektronske pošte se je treba zavedati, da **(nekriptirana) elektronska pošta ni zanesljivo varen način prenosa podatkov**, čeprav se v praksi prestrezanje teh vsebin ne dogaja pogosto. Drugače pa je pri tako imenovanih ponudnikih »brezplačniške« elektronske pošte (Gmail, Yahoo ...), kjer z uporabo soglašamo tudi z vpogledom v našo korespondenco.

Zaradi tega bi priporočali, da **se za komunikacijo med učitelji in učenci uporabljajo šolski elektronski naslovi oziroma naslovi evropskih ponudnikov**. To je še toliko bolj pomembno, če je elektronska pošta uporabljena za prenos vsebin, ki vključujejo tudi osebne podatke.

**Elektronska pošta ni namenjena prenosu zelo velikih datotek**, zato je take datoteke smiselno deliti v spletnih učilnicah. V primeru, da šola ne uporablja spletnih učilnic, pa je priporočljiva uporaba varnih specializiranih orodij, kot je na primer Arnesov Filesender.

## Spletna stran šole

Mnoge šole so spomladi uporabljale kar svojo spletno stran za obveščanje učencev in staršev in za deljenje nekaterih gradiv. Pri tem je zelo pomembno, da je spletna stran šole **postavljena v dobro varovanem okolju**, da ne pride do okužbe, vdora ali pa do razobličenja šolske strani.

## Video konference

Pri uporabi vseh video konferenc je pomembno, da **se zavedamo možnosti zlorab** in tam, kjer je to možno, uporabljamo gesla za dostop v konference, predvsem pa moramo učencem sporočiti, da je deljenje konferenčne povezave izredno tvegano početje in da s tem, ko povezavo z nekom delijo, lahko nepovabljenim omogočijo vstop v našo video učilnico.

Pri video konferencah je **lahko problematično tudi snemanje in pa prisotnost nepovabljenih oseb, ki so lahko v prostoru skupaj z učencem**. Tu bi opozorili na to, da mora učitelj oziroma šola postaviti jasna pravila glede tega, ali je pri takem pouku dovoljena prisotnost staršev ali ne in ali je dovoljeno snemanje konferenc in če je, pod kakšnimi pogoji.

## Spletne učilnice

To pomlad se je zelo razširila uporaba spletnih učilnic. Pri tem se je dogajalo, da so se za dostop v učilnice za mlajše učence uporabili kar elektronski naslovi staršev. V takem primeru je treba starše opozoriti na to, da so lahko s tem njihovi elektronski naslovi vidni tudi drugim, ki dostopajo do učilnice. Priporočljivo pa bi bilo, da šola vsem učencem s soglasjem staršev za otroke oz. najstnike mlajše od 16 let, dodeli šolske elektronske naslove, pri čemer jih lahko mlajši otroci uporabljajo ob pomoči staršev.

## Deljenje povezav do spletnih vsebin

Preden delimo neko hiperpovezavo, jo je vedno treba ponovno preveriti, saj se nam lahko sicer zgodi, da je prišlo do vdora v stran, ki smo jo delili ali pa - kar je bolj običajno – da je domena, pod katero je bila stran postavljena, potekla in jo je ponudnik uporabil za nekoga drugega ali pa nanjo postavil neko začasno, pogosto tudi neprimerno vsebino.

## Priporočene spletne strani

Ta priporočila so splošne narave, za vse aktualne informacije pa vam svetujemo, da redno sledite objavam na slovenskem šolskem portalu SIO, na straneh SAFE.SI in na straneh projekta Varni na internetu.

Več informacij o varni rabi interneta in izvajanju pouka na daljavo boste našli na:

 <p>Center za varnejši internet</p> <p><a href="http://www.safe.si">www.safe.si</a></p>	 <p><b>VARNI NA INTERNETU</b> Od mene je odvisno vse.</p> <p><a href="http://www.varninainternetu.si">www.varninainternetu.si</a></p>	 <p><b>LOGOUT</b> Center pomoči pri prekomerni rabi interneta</p> <p><a href="http://www.logout.si">www.logout.si</a></p>
--	--	--



V primeru, da se vaši učenci oz. dijaki znajdejo v težavah pri uporabi interneta, pa se lahko vedno obrnejo na Tom telefon: [www.e-tom.si](http://www.e-tom.si). Prav tako lahko tudi starši poiščejo pomoč na Tom telefonu, če se njihov otrok ali najstnik znajde v težavah pri uporabi spleta.

V primeru, da družina potrebuje pomoč pri vzpostavitvi družinskih pravil glede uporabe interneta, pri težavah s prekomerno rabo interneta, in pri težavah s spletnim nasiljem, se lahko obrne na Logout ([www.logout.si](http://www.logout.si)).

## Storitve in izobraževanja, ki jih šolam, učiteljem in staršem ponuja ARNES

- Pregled storitev za šole, učitelje in učence ter dijake: [www.arnes.si/storitve](http://www.arnes.si/storitve)
- Izobraževanja za učitelje, starše, učence ter dijake: [www.arnes.si/izobrazevanje](http://www.arnes.si/izobrazevanje)
- SIO portal, kjer bodo učitelji našli veliko aktualnih informacij za svoje delo: [sio.si](http://sio.si)
- SIO webinarji in izobraževanja: [izobrazevanje.sio.si](http://izobrazevanje.sio.si)
- E-poštne novice ARNES informator: [informator.arnes.si](http://informator.arnes.si)